(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000228060 A**

(43) Date of publication of application: **15.08.00**

(51) Int. Cl **G11B 20/10**
G06F 12/14
G09C 1/00
H04L 9/10
H04N 5/91
H04N 5/92

(21) Application number: **11144928**

(22) Date of filing: **25.05.99**

(30) Priority: **02.12.98 JP 10343013**

(71) Applicant: **OLYMPUS OPTICAL CO LTD**

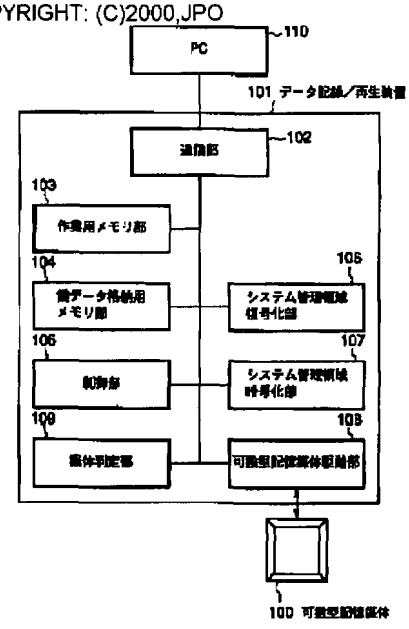
(72) Inventor: **KONDO TAKASHI**

(54) **DATA RECORDING/REPRODUCING DEVICE USING PORTABLE STORAGE MEDIUM**

(57) Abstract:

PROBLEM TO BE SOLVED: To secure the securecy and the genuineness of data by holding encryption secret information including an encryption key signal or an encryption key generating information for generating an encryption key signal and performing the cryptographic processing of data for system management while using the encryption secret information and recording the ciphered data for system management in the system management area of a storage medium.

SOLUTION: When the data received from an external PC 110 via a communication part 102 are written on a portable storage medium 100, data for system management are read out in a memory part for work 103. The data received from the external PC 110 are written on the medium 103 by using decoded data for system management. Since the constitution of the data on the medium 100 is updated, the data for system management on the memory for work 103 are also updated. The data for system management on the memory for work 103 are ciphered by using a ciphering part 107 and the ciphered data for system management are written in the system management area of the medium 100 by using a portable storage medium driving part 108.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（A）**　(11)特許出願公開番号
特開2000－228060
（P2000－228060A）
(43)公開日　平成12年８月15日(2000.8.15)

(51)Int.Cl.'	識別記号	FI	テーマコード'(参考)
G11B 20/10		G11B 20/10	H
G06F 12/14	320	G06F 12/14	320B
G09C 1/00	660	G09C 1/00	660D
H04L 9/10		H04L 9/00	621Z
H04N 5/91		H04N 5/91	P

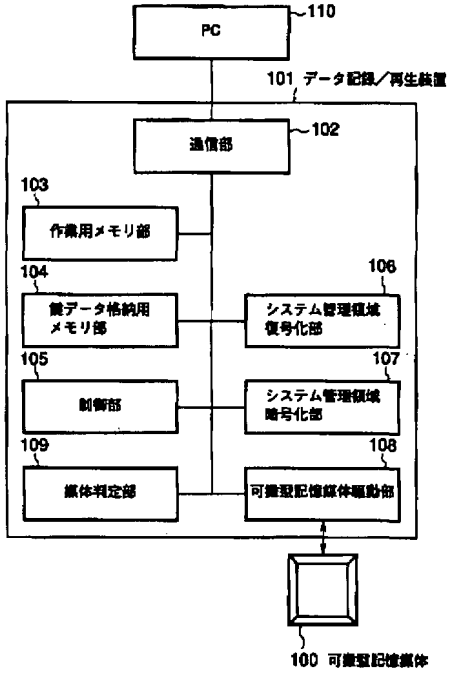
審査請求　未請求　請求項の数18　ＯＬ　（全 32 頁）　最終頁に続く

(21)出願番号　特願平11－144928
(22)出願日　平成11年５月25日(1999.5.25)
(31)優先権主張番号　特願平10－343013
(32)優先日　平成10年12月２日(1998.12.2)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000000376
オリンパス光学工業株式会社
東京都渋谷区幡ヶ谷２丁目43番２号
(72)発明者　近藤　隆
東京都渋谷区幡ヶ谷２丁目43番２号　オリンパス光学工業株式会社内
(74)代理人　100058479
弁理士　鈴江　武彦　（外４名）

(54)【発明の名称】　可搬型記憶媒体を用いたデータ記録／再生装置

(57)【要約】
【課題】本発明は、大容量の画像データ等を可搬型記憶媒体に格納する際、データ内容の秘匿性、真正性を確保し、且つデータの不正な消去・破壊を含めた改竄を防止でき、且つ高速な処理を実現できるデータ記録／再生装置を提供する。
【解決手段】本発明の一態様によると、システム管理用データが記録されるシステム管理領域及びユーザー用データが記録されるユーザー領域を有する可搬型記憶媒体にデータを記録するデータ記録装置において、暗号化鍵信号又は暗号化鍵信号を生成するための暗号化鍵信号生成情報を含む暗号化秘密情報を保持する暗号化秘密情報保持手段と、前記暗号化秘密情報保持手段に保持されている前記秘密情報暗号化を用いて暗号化処理を行う暗号化手段と、前記暗号化手段により、前記可搬型記憶媒体のシステム管理領域に記録すべきシステム管理用データの少なくとも一部を暗号化処理して前記可搬型記憶媒体のシステム管理領域へ記録する記録手段とを有することを特徴とするデータ記録装置が提供される。



【特許請求の範囲】

【請求項１】　システム管理用データが記録されるシステム管理領域及びユーザー用データが記録されるユーザー領域を有する可搬型記憶媒体にデータを記録するデータ記録装置において、

暗号化鍵信号又は暗号化鍵信号を生成するための暗号化鍵信号生成情報を含む暗号化秘密情報を保持する暗号化秘密情報保持手段と、

前記暗号化秘密情報保持手段に保持されている前記暗号化秘密情報を用いて暗号化処理を行う暗号化手段と、

前記暗号化手段により、前記可搬型記憶媒体のシステム管理領域に記録すべきシステム管理用データの少なくとも一部を暗号化処理して前記可搬型記憶媒体のシステム管理領域へ記録する記録手段と、

を有することを特徴とするデータ記録装置。

【請求項２】　前記暗号化手段は、前記可搬型記憶媒体のユーザー領域へユーザー用データの書き込む処理を行っているときに、時間的に、並行して前記可搬型記憶媒体のシステム管理領域に記録すべきシステム管理用データの少なくとも一部の前記暗号化処理を行うことを特徴とする請求項１記載のデータ記録装置。

【請求項３】　システム管理用データが記録されるシステム管理領域及びユーザー用データが記録されるユーザー領域を有する可搬型記憶媒体からデータを読み出すデータ再生装置において、

復号化鍵信号又は復号化鍵信号を生成するための復号化鍵信号生成情報を含む復号化秘密情報を保持する復号化秘密情報保持手段と、

前記復号化秘密情報保持手段に保持されている前記復号化秘密情報を用いて復号化処理を行う復号化手段と、

前記復号化手段により、前記可搬型記憶媒体のシステム管理領域にシステム管理用データの少なくとも一部が前記暗号化秘密情報を用いて暗号化して記録されている前記可搬型記憶媒体のシステム管理領域から前記暗号化されて記録されている前記システム管理用データを読み出し、前記復号化手段を用いて前記暗号化して記録されているシステム管理用データの少なくとも一部を復号するシステム管理用データ再生手段と、

を有することを特徴とするデータ再生装置。

【請求項４】　前記記録手段は、

前記可搬型記録媒体にユーザー用データを記録する際に、このユーザー用データを可搬型記録媒体上で論理的にアクセス可能な単位領域のサイズに分割するデータ分割手段と、

前記可搬型記録媒体のユーザー領域から未使用の単位記録領域を選択する記録領域選択手段と、

前記記録領域選択手段によって選択された複数の未使用の単位記録領域の内の隣接する各領域に対して、前記分割手段によって分割されたデータが不規則な配置で記録されるように、分割されたデータの記録を制御する記録制御手段と、

を有することを特徴とする請求項１記載のデータ記録装置。

【請求項５】　前記記録手段は、

前記可搬型記録媒体を初期化する処理の際に、前記可搬型記録媒体の複数の単位記録領域の内、少なくとも１つの単位領域を欠陥領域として前記システム管理用データに登録する欠陥領域登録手段、

を有することを特徴とする請求項１記載のデータ記録装置。

【請求項６】　前記記録手段は、

任意性のあるパラメータを用いてランダムなデータを生成するランダムデータ生成手段と、

前記可搬型記録媒体を初期化する際に、前記ランダムデータ生成手段によって得られたランダムデータを前記可搬型記録媒体のユーザー領域全体に書き込むランダムデータ書き込み手段と、

前記パラメータを前記可搬型記録媒体のシステム管理領域に記録するパラメータ記録手段と、

を有することを特徴とする請求項１記載のデータ記録装置。

【請求項７】　前記ランダムデータ書き込み手段は、

前記可搬型記録媒体からデータを削除する際に、前記可搬型記録媒体のデータ削除領域に前記ランダムデータを再度書き込むものであることを特徴とする請求項６記載のデータ記録装置。

【請求項８】　前記記録手段は、

任意性のあるパラメータを用いてランダムなデータを生成するランダムデータ生成手段と、

前記可搬型記録媒体のユーザー領域から未使用の領域を複数選択する未使用領域選択手段と、

前記未使用領域選択手段により得られた領域に前記ランダムなデータを書き込むランダムデータ書込手段と、

を有することを特徴とする請求項１記載のデータ記録装置。

【請求項９】　前記記録手段は、

前記ユーザー用データを前記ユーザー領域の連続する単位記録領域に従つて連続して記録するものであり、

前記連続する単位記録領域の内、先頭及び最後尾の単位記録領域ＩＤと、前記単位記録領域内の欠陥領域ＩＤとを、前記システム管理領域のファイル管理用テーブルに記録するＩＤ記録手段と、

前記ファイル管理用テーブルに記録されたＩＤに基づき、前記可搬型記録媒体上に記録された前記ユーザー用データの物理的なアドレスを求めるアドレス手段と、

を有することを特徴とする請求項１記載のデータ記録装置。

【請求項１０】　前記記録手段は、

前記ユーザー用データの少なくとも一部に対して、所定の処理を施す処理手段と、

前記処理手段により所定の処理が施された領域のデータ上のアドレス、該アドレスに関連する情報、及び前記所定の処理に必要なパラメータの内の少なくとも一つを前記システム管理用データに記録する処理情報記録手段と、
を有することを特徴とする請求項９記載のデータ記録装置。
【請求項１１】　前記処理手段は、
各単位記録領域内のデータ単位でシャッフルを行うことを特徴とする請求項１０記載のデータ記録装置。
【請求項１２】　前記処理手段は、
各単位記録領域単位でシャッフルを行うことを特徴とする請求項１０記載のデータ記録装置。
【請求項１３】　前記処理手段は、
前記ユーザー用データの全体に対するシヤッフルを行うことを特徴とする請求項１０記載のデータ記録装置。
【請求項１４】　前記処理手段は、
データを暗号化する処理を行うことを特徴とする請求項１０記載のデータ記録装置。
【請求項１５】　前記処理手段は、
単位領域内シヤッフル、単位記録領域単位シヤッフル、前記ユーザー用データの全体に対するシャッフル、及びデータ暗号化の処理の内から少なくとも二つの処理を組み合わせて行うことを特徴とする請求項１０記載のデータ記録装置。
【請求項１６】　前記記録手段は、
前記可搬型記録媒体に記録されるユーザー用データから抽出して得られる所定のコードを前記システム管理領域に記録するコード抽出記録手段、
を有することを特徴とする請求項１記載のデータ記録装置。
【請求項１７】　前記ユーザー用データ再生手段は、
前記可搬型記録媒体から読み出した前記ユーザー用データから所定のコードを抽出するコード抽出手段と、
このコード抽出手段により抽出されたコードと、前記可搬型記録媒体に前記ユーザー用データを記録する際に抽出され前記システム管理領域に予め記録されている前記コードとを前記照合するコード照合手段と、
を有することを特徴とする請求項３記載のデータ再生装置。
【請求項１８】　前記ユーザー用データ再生手段は、
前記システム管理領域から前記パラメータを読み出すパラメータ読み出し手段と、
前記システム管理領域から読み出したパラメータを用いて生成したランダムデータと、前記可搬型記録媒体の未使用領域のクラスタに記載されているランダムデータとを照合する手段と、
を有することを特徴とする請求項３記載のデータ再生装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、例えば、光磁気ディスク（ＭＯ）等の可搬型記憶媒体にデータを暗号化して記録すると共に、暗号化して記録されたデータを再生するデータ記録／再生装置及びデータを暗号化して可搬型記憶媒体に記録する際に予め可搬型記憶媒体への不正なアタックに対する防御対策を伴って記録／再生するようにしたデータ記録／再生装置に関する。
【０００２】
【従来の技術】周知のように、デジタル画像等のコンテンツに対し、その内容の秘匿性、真正性（改竄されていないこと）を確保するための技術は、従来から幾つか提案されている。
【０００３】例えば、特公平７－１２２９６０号公報には、デジタルカメラ内に乱数発生装置を設け、デジタルカメラで撮影された画像に対し、デジタルカメラ内で前記乱数系を用いて画像データを暗号化することにより、画像内容の秘匿性や真正性を確保するという手法が開示されている。
【０００４】また、特開平９－２００７３０号公報には、カメラ内で画像データの電子署名を作成することにより、画像データが改竄されているかどうかを検知することができる手法が開示されている。
【０００５】また、光磁気デイスクを用いた医療画像の電子保存システムであるＩＳ&Ｃ（Ｉｍａｇｅ　Ｓａｖｅ　＆　Ｃａｒｒｙ）システム（参考資料「画像の電子保管とＩＳ&Cシステム」、新医療１９９４年７月号Ｐ３６－４０）では、光磁気ディスクのファイルシステムやデバイスドライバを特殊化すると共に、専用のソフトウェア（データの改変が不可）以外ではアクセスできないようにすることにより、デジタル画像等のコンテンツの秘匿性、真正性を確保している。
【０００６】
【発明が解決しようとする課題】しかしながら、前者の特公平７－１２２９６０号公報や特開平９－２００７３０号公報による手法では、画像内容の漏洩という脅威からコンテンツを保護することは可能であるが、悪意あるユーザーが汎用の計算機等を用いて画像ファイルにアクセスして画像ファイルを消去したり、データ内容を破壊する脅威、すなわち広い意味での画像内容の改竄から、コンテンツを守ることはできない。
【０００７】また、デジタルカメラで撮影される画像は１００万画素を越える大きさであり、このような大きなサイズの画像データを暗号化したり、画像データから電子署名を求めたりする演算量は非常に大きくなり、処理時間も長くなってしまう。
【０００８】特に、デジタルカメラの内部で暗号等の処理を行おうとすると、内部のＣＰＵの処理能力はそれほど大きなものが期待できないため、処理時間は無視できないほど長くなってしまう。

【0009】この問題は、デジタルカメラに連写機能を備える場合などに顕著になる。

【0010】また、デジタルビデオカメラ装置のように、動画のデータとなると、さらにデータサイズが大きくなるため、処理時間の問題はさらに深刻になる。

【0011】一方、後者のＩＳ&Ｃシステムのような専用のファイルシステムでは、データ暗号化の処理を必要としないので処理時間は問題にならない。

【0012】しかし、ファイルシステムの構造が漏洩してしまった場合には、ある程度保存装置等の知識のあるユーザーなら、可搬型記憶媒体上のファイルにアクセスできてしまう。

【0013】また、暗号化の手法を使った場合のように、可搬型記憶媒体上のファイルの安全性を守るための情報が漏洩した場合に、暗号化の鍵だけを取りかえれば済むというようなことはできない。

【0014】さらには、データ内容の安全性確保のための装置としては、むしろ安全性確保のための機構を公開した上でも安全性を確保できることが望ましい。

【0015】本発明はこれらの点に着目し、画像等の大容量のデータを可搬型記憶媒体に格納する場合に、データ内容の秘匿性、真正性を確保し、且つデータの不正な消去・破壊を含めた改竄を防止でき、且つ高速な処理を実現できるデータ記録／再生装置を提供することを目的とする。

【0016】

【課題を解決するための手段】本発明によると、上記課題を解決するために、（１）　システム管理用データが記録されるシステム管理領域及びユーザー用データが記録されるユーザー領域を有する可搬型記憶媒体にデータを記録するデータ記録装置において、暗号化鍵信号又は暗号化鍵信号を生成するための暗号化鍵信号生成情報を含む暗号化秘密情報を保持する暗号化秘密情報保持手段と、前記暗号化秘密情報保持手段に保持されている前記暗号化秘密情報を用いて暗号化処理を行う暗号化手段と、前記暗号化手段により、前記可搬型記憶媒体のシステム管理領域に記録すべきシステム管理用データの少なくとも一部を暗号化処理して前記可搬型記憶媒体のシステム管理領域へ記録する記録手段と、を有することを特徴とするデータ記録装置が提供される。

【0017】また、本発明によると、上記課題を解決するために、（２）　前記前記暗号化手段は、前記可搬型記憶媒体のユーザー領域へユーザー用データの書き込む処理を行っているときに、時間的に、並行して前記可搬型記憶媒体のシステム管理領域に記録すべきシステム管理用データの少なくとも一部の前記暗号化処理を行うことを特徴とする（１）記載のデータ記録装置が提供される。

【0018】また、本発明によると、上記課題を解決するために、（３）　システム管理用データが記録されるシステム管理領域及びユーザー用データが記録されるユーザー領域を有する可搬型記憶媒体からデータを読み出すデータ再生装置において、復号化鍵信号又は復号化鍵信号を生成するための復号化鍵信号生成情報を含む復号化秘密情報を保持する復号化秘密情報保持手段と、前記復号化秘密情報保持手段に保持されている前記復号化秘密情報を用いて復号化処理を行う復号化手段と、前記復号化手段により、前記可搬型記憶媒体のシステム管理領域にシステム管理用データの少なくとも一部が前記暗号化秘密情報を用いて暗号化して記録されている前記可搬型記憶媒体のシステム管理領域から前記暗号化されて記録されている前記システム管理用データを読み出し、前記復号化手段を用いて前記暗号化して記録されているシステム管理用データの少なくとも一部を復号するシステム管理用再生手段と、を有することを特徴とするデータ再生装置が提供される。

【0019】（作用効果）上記（１）又は（３）の発明では、予めデータ記録装置内に暗号化又は復号化を行うための暗号化鍵又は復号化鍵（秘密鍵方式の暗号アルゴリズムを用いる場合は、暗号化鍵と復号化鍵は同じ）、もしくは暗号化鍵や復号化鍵を生成するための秘密情報を格納しておき、可搬型記憶媒体にデータを記録する場合に、可搬型記憶媒体上のシステム管理領域に記録されているルートデイレクトリテーブルのエントリーデータや可搬型記憶媒体上の物理的アドレスと論理的アドレスを対応づける情報が格納されたデータを前記暗号化鍵で暗号化して記録する。

【0020】このようにすることにより、汎用のデータ記録／再生装置で前記可搬型記憶媒体にアクセスしようとしても、汎用の装置ではデータファイルにアクセスするための情報を読み出すことができないため、データにアクセスできない。

【0021】また、ユーザーがデータ保存装置に対する知識が深く、例えば、ＳＣＳＩ（Ｓｍａｌｌ　Ｃｏｍｐｕｔｅｒ　Ｓｙｓｔｅｍ　Ｉｎｔｅｒｆａｃｅ）などの低レベルなコマンドを使って、上記データファイルにアクセスするための情報を読み出しても、暗号化の鍵を知らない限り、アクセスするための情報を解読することは極めて困難なため、データにアクセスすることは実際上できない。

【0022】さらに、本発明による手法では、暗号化するのは可搬型記憶媒体のシステム管理領域に記録されているデータであり、例えば、システム管理用域のデータ全体を暗号化するとしても、このデータのサイズは、画像データや動画像データに比べるとはるかに小さいため、暗号化の演算を施すための処理時間は少なくて済むことになる。

【0023】例えば、１３０万画素の画像データを圧縮せずにファイルに保存すると、約４メガバイトのデータサイズになるが、一方で１ギガバイトのディスクでも、

システム管理領域のデータサイズは高々数百キロバイトである。

【0024】つまり、システム管理領域のデータを暗号化するのに比べ、画像データを暗号化しようとすると、上記の例では数百倍の演算量を必要とすることになる。

【0025】データサイズが数百メガバイト～数ギガバイトにもなる動画データになると、この差はさらに顕著になる。

【0026】また、上記（2）の発明では、面像等のデータを可搬型記憶媒体中に書き込んでいる時間に並行してシステム管理用データの暗号化処理を行うことにより、暗号化の処理時間によるストレスを解消する。

【0027】通常、可搬型記憶媒体へデータを書き込む処理には専用のプロセッサが用いられ、そのため暗号化の処理を行うためのプロセッサ（例えば、CPU）とは異なる。

【0028】また、画像データ等の可搬型記憶媒体への書き込みとシステム管理領域のデータを暗号化する処理を並列に行ってもデータ的な問題は起こらない。

【0029】画像や動画像のデータは数メガバイト～数百メガバイトに達し、データ書き込みにある程度時間を必要とする。

【0030】したがって、データ書き込み時にシステム管理領域のデータを暗号化する処理を並行に行うことにより、暗号化による処理時間のストレスをなくすことが可能となる。

【0031】なお、上記（1）乃至（3）の発明は後述する第1の実施の形態が対応し、関連する図は図1乃至図10である。

【0032】また、本発明によると、上記課題を解決するために、（4）　前記記録手段は、前記可搬型記録媒体にユーザー用データを記録する際に、このユーザー用データを可搬型記録媒体上で論理的にアクセス可能な単位領域のサイズに分割するデータ分割手段と、前記可搬型記録媒体のユーザー領域から未使用の他に記録領域を選択する記録領域選択手段と、前記記録領域選択手段によって選択された複数の未使用の単位記録領域の内の隣接する各領域に対して、前記分割手段によって分割されたデータが不規則な配置で記録されるように、分割されたデータの記録を制御する記録制御手段と、を有することを特徴とする（1）記載のデータ記録装置が提供される。

【0033】この（4）の発明は後述する第2の実施の形態が対応し、関連する図は図12及び図15乃至図17である。

【0034】そして、この（4）の発明中の論理的にアクセス可能な単位領域とは、FATファイルシステムなどで言うところのクラスタ領域に対応する。

【0035】図15は、データが記録されるときに、ID=3，12，14，19に対応するハッチングされた領域で示すデータをクラスタのサイズで分解し、それを連続しないクラスタに記録する概念図を示している。

【0036】従って、この場合、ID=2，4，13，18に対応する白抜き領域で示すデータはクラスタのサイズで分解されないものとしている。

【0037】（作用効果）通常のファイルシステムでは、データを記録する場合、ユーザー領域内で物理的にほぼ連続した領域へ記録する。

【0038】したがって、上記（1）乃至（3）の発明だけでは、ユーザー領域に直接アクセスしてユーザー領域に記録されているビットパターンを解析することで、記録されているデータの内容が不正に読み出されてしまうという恐れがある。

【0039】これに対し、この（4）の発明では、データを記録する場合には、まず、データを複数に分割し、その後、分割された各データ同士が物理的に不連続になるようにユーザー領域に記録する。

【0040】したがつて、ユーザー領域へ直接アクセスして記録されているビットパターンを読み出しても、そこから元のデータを復元することは困難である。

【0041】例として、可搬型記録媒体として、総容量1ギガバイト、クラスタサイズ16キロバイトのディスクに、6メガバイト（200万画素非圧縮の画像データに相当）のデータを記録する場合を考える。

【0042】この場合、ディスク全体のクラスタ総数は62500個であり、また、6メガバイトのファイルを構成するクラスタ数は375個であるので、可能なデータの順序付の組み合わせ数Cは、データサイズが既知の場合でも、

C=65200！／（65200－375）！

であるから、Cは、ほぼ65200^{375} 通りも存在し、総当たり的に元のデータを解読することは実際上不可能である。

【0043】また、本発明によると、上記課題を解決するために、（5）　前記記録手段は、前記可搬型記録媒体を初期化する処理の際に、前記可搬型記録媒体の複数の単位記録領域の内、少なくとも一つの単位領域を欠陥領域として前記システム管理用データに登録する欠陥領域登録手段、を有することを特徴とする（1）記載のデータ記録装置が提供される。

【0044】この（5）の発明は後述する第2の実施の形態が対応し、関連する図は図18及び図19である。

【0045】（作用効果）この（5）の発明によれば、ユーザー領域内にデータを記録できない欠陥領域を複数配置する（FATファイルシステムの場合では、FATエントリの一部に欠陥クラスタであることを示すコードを記録する）ことで、データを記録する際に記録媒体上での連続性を低下させ、その結果、ユーザー領域に直接アクセスしてユーザー領域に記録されているビットパターンを解析することでデータが不正に読み出されてしま

うという危険性を下げることができる。

【００４６】また、この（５）の発明では、媒体初期化時に欠陥領域を記録する以外は、上記（１）乃至（３）の発明の処理と同じであるという構造の単純さと、処理が軽いというメリットがある。

【００４７】また、本発明によると、上記課題を解決するために、（６）　前記記録手段は、任意性のあるパラメータを用いてランダムなデータを生成するランダムデータ生成手段と、前記可搬型記録媒体を初期化する際に、前記ランダムデータ生成手段によって得られたランダムデータを前記可搬型記録媒体のユーザー領域全体に書き込むランダムデータ書き込み手段と、前記パラメータを前記可搬型記録媒体のシステム管理領域に記録するパラメータ記録手段と、を有することを特徴とする（１）記載のデータ記録装置が提供される。

【００４８】また、本発明によると、上記課題を解決するために、（７）　前記ランダムデータ書き込み手段は、前記可搬型記録媒体からデータを削除する際に、前記可搬型記録媒体のデータ削除領域に前記ランダムデータを再度書き込むものであることを特徴とする（６）記載のデータ記録装置が提供される。

【００４９】この（６）及び（７）の発明は後述する第２の実施の形態が対応し、関連する図は図２０乃至図２２である。

【００５０】（作用効果）通常、可搬型記録媒体の初期化（出荷）時には、ユーザー領域は均一の値（各ビットがが全てＯＮ、あるいはすべてＯＦＦ）となっている。

【００５１】したがって、可搬型記録媒体上に少数のデータしか記録されていない場合には、上記（４）の発明で述べたような総当たり的アタックに対して組み合わせの数が少なくなるためデータの安全性の度合いが低くなる。

【００５２】しかるに、この（６）及び（７）の発明によると、可搬型記録媒体のユーザー領域は、可搬型記録媒体の初期化時にランダムな値が記録されているため、媒体上に少数のデータしか記録されていない場合でも、記録されていない領域のビットのＯＮ／ＯＦＦが一様でないため、アタックするためには総当たり的な手法が必要になり、データの安全性が向上する。

【００５３】また、本発明によると、上記課題を解決するために、（８）　前記記録手段は、任意性のあるパラメータを用いてランダムなデータを生成するランダムデータ生成手段と、前記可搬型記録媒体のユーザー領域から未使用の領域を複数選択する未使用領域選択手段と、前記未使用領域選択手段により得られた領域に前記ランダムなデータを書き込むランダムデータ書込手段と、を有することを特徴とする（１）記載のデータ記録装置が提供される。

【００５４】この（８）の発明は後述する第２の実施の形態が対応し、関連する図は図２０及び図２３である。

【００５５】（作用効果）可搬型記録媒体のユーザー領域にデータを書き込む前からデータを改竄することを意図するならば、データを書き込む前のユーザー領域のビットパターンを全部ダンプして記録しておき、書き込んだ後に再びユーザー領域のビットパターンをすべてダンプし、両方のビットパターンを比較して差分をとると、書き込んだデータが記録されている領域の特定ができてしまう。

【００５６】したがって、可搬型記録媒体上に少数のデータしか記録されていない場合には、上記（４）の発明で述べたような総当たり的アタックに対して組み合わせの数が少なくなるためデータの安全性の度合いが低くなる。

【００５７】しかるに、この（８）の発明によると、可搬型記録媒体のユーザー領域にデータを書き込むとき、同時にダミーのデータを実際に記録したいデータと共に書き込むことで、上記のアタックに対してデータの安全性が向上する。

【００５８】また、本発明によると、上記課題を解決するために、（９）　前記記録手段は、前記ユーザー用データを前記ユーザー領域の連続する単位記録領域に従つて連続して記録するものであり、前記連続する単位記録領域の内、先頭及び最後尾の単位記録領域ＩＤと、前記単位記録領域内の欠陥領域ＩＤとを、前記システム管理領域のファイル管理用テーブルに記録するＩＤ記録手段と、前記ファイル管理用テーブルに記録されたＩＤに基づき、前記可搬型記録媒体上に記録された前記ユーザー用データの物理的なアドレスを求めるアドレス手段と、を有することを特徴とする（１）記載のデータ記録装置が提供される。

【００５９】この（９）の発明は後述する第２の実施の形態が対応し、関連する図は図２４及び図２５である。

【００６０】（作用効果）例えば、高精細のデジタルカメラ等で撮影されたデータのサイズは一般に大きく、したがって、その撮影データを可搬型記録媒体に記録するときに使用するＦＡＴエントリの個数も大きくなる。

【００６１】前述したように、クラスタサイズ１６キロバイトのディスクへ６メガバイト（２００万画素非圧縮の両像データに相当）のデータを記録する場合、３７５個のＦＡＴエントリが必要になる。

【００６２】そして、ＦＡＴのエントリが大きくなれば、上記（１）乃至（３）の発明における暗号化／復号化処理の負担が大きくなる。

【００６３】一方、データを記録するときに、データが書き込まれる先頭位置と最後尾の位置が分かるような情報をシステム管理領域に記録することでもデータにアクセスすることは可能である。

【００６４】この場合、必要なＦＡＴエントリの数は最少２個で済むが、データを記録する領域中に欠陥クラスタがあれば、その位置及び個数を記録しなければならな

いので、その分必要なエントリの数が増えるが、通常ほとんどゼロであるので、1つの画像をユーザー領域に書き込むときに必要なＦＡＴエントリの数は、データが書き込まれる先頭位置と最後尾の位置が分かるような情報、及び書き込む領域内に存在する欠陥クラスタの個数を表す情報の3つである。

【００６５】したがって、前述の6メガバイトのデータを書き込む場合、必要になるＦＡＴエントリの個数は１００分の1以下になる。

【００６６】このことは、データ再生装置の暗号化／復号化の処理速度向上のために、非常に有効な手段となる。

【００６７】また、本発明によると、上記課題を解決するために、（１０）　前記記録手段は、前記ユーザー用データの少なくとも一部に対して、所定の処理を施す処理手段と、前記処理手段により所定の処理が施された領域のデータ上のアドレス、該アドレスに関連する情報、及び前記所定の処理に必要なパラメータの内の少なくとも一つを前記システム管理用データに記録する処理情報記録手段と、を有することを特徴とする（９）記載のデータ記録装置が提供される。

【００６８】この（１０）の発明は後述する第２の実施の形態が対応し、関連する図は図２４乃至図２７である。

【００６９】また、本発明によると、上記課題を解決するために、（１１）　前記処理手段は、各単位記録領域内のデータ単位でシャッフルを行うことを特徴とする（１０）記載のデータ記録装置が提供される。

【００７０】この（１１）の発明は後述する第２の実施の形態が対応し、関連する図は図２４乃至図２８及び図３０である。

【００７１】また、本発明によると、上記課題を解決するために、（１２）　前記処理手段は、各単位記録領域単位でシャッフルを行うことを特徴とする（１０）記載のデータ記録装置が提供される。

【００７２】この（１２）の発明は後述する第２の実施の形態が対応し、関連する図は図２４乃至図２９である。

【００７３】また、本発明によると、上記課題を解決するために、（１３）　前記処理手段は、前記ユーザー用データの全体に対するシヤッフルを行なうことを特徴とする（１０）記載のデータ記録装置が提供される。

【００７４】この（１３）の発明は後述する第２の実施の形態が対応し、関連する図は図２４乃至図２８及び図３１である。

【００７５】また、本発明によると、上記課題を解決するために、（１４）　前記処理手段は、データを暗号化する処理を行うことを特徴とする（１０）記載のデータ記録装置が提供される。

【００７６】この（１４）の発明は後述する第２の実施の形態が対応し、関連する図は図２４乃至図２７及び図３２である。

【００７７】また、本発明によると、上記課題を解決するために、（１５）　前記処理手段は、単位領域内シヤッフル、単位記録領域単位シヤッフル、前記ユーザー用データの全体に対するシャッフル、及びデータ暗号化の処理の内から少なくとも二つの処理を組み合わせて行うことを特徴とする（１０）記載のデータ記録装置が提供される。

【００７８】この（１５）の発明は後述する第２の実施の形態が対応し、関連する図は図２４乃至図２８及び図３０、図３２である。

【００７９】（作用効果）上記（９）の発明では、データをユーザー領域上で連続的に記録することを前提としている。

【００８０】したがって、このままでは、ユーザー領域に直接アクセスしてユーザー領域に記録されているビットパターンを解析することで、そこに記録されているデータの内容を不正に読み出されてしまうという恐れがある。

【００８１】そこで、（１０）の発明では、データを記録するときに、そのまま記録するのではなく、データをシヤッフルしたり暗号化する等の処理を施して記録することをでデータの安全性を高める処理を施す。

【００８２】この際に、シャッフルや暗号化の処理に必要なパラメータを上記（９）の発明のＦＡＴエントリ中に図２６に示すようにして埋め込めば、データ毎にデータを保護するための様々な処理バリエーションを加えることが可能となり、且つ、上記（９）の発明の効果であるＦＡＴのサイズを小さくできるという効果も得ることができる。

【００８３】また、（１１）乃至（１５）の発明は、データの安全性を高めるための処理を行うものである。

【００８４】また、本発明によると、上記課題を解決するために、（１６）　前記記録手段は、前記可搬型記録媒体に記録されるユーザーデータから抽出して得られる所定のコードを前記システム管理領域に記録するコード抽出記録手段、を有することを特徴とする（１）記載のデータ記録装置が提供される。

【００８５】また、本発明によると、上記課題を解決するために、（１７）　前記システム管理用データ再生手段は、前記可搬型記録媒体から読み出した前記ユーザー用データから所定のコードを抽出するコード抽出手段と、このコード抽出手段により抽出されたコードと、前記可搬型記録媒体に前記ユーザー用データを記録する際に抽出され前記システム管理領域に予め記録されている前記コードとを前記照合するコード照合手段と、を有することを特徴とする（３）記載のデータ再生装置が提供される。

【００８６】この（１６）及び（１７）の発明は後述す

る第2の実施の形態が対応し、関連する図は図34乃至図38である。

【0087】（作用効果）上記（10）乃至（15）の発明が記録するデータをスクランブルしてデータを読めなくすることでデータの安全性を確保する発明であったのに対し、この（16）及び（17）の発明ならびに後述する（18）の発明はデータを読み出すことは可能だが、改竄すると改竄したことがわかるような仕組みを施すことでデータの安全性を確保する発明である。

【0088】この場合、基本的な考え方としては、通信等で用いられているメッセージ認証子（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ：MAC）の方法に基づいている。

【0089】以下に、このMACの方法を説明する。

【0090】MACを用いてデータの改竄を検知する方法では、まず、データに所定の演算（通常、方向性関数であるHASH関数（ハッシュ値）が用いられる）を施してメッセージ・ダイジェスト（MD）と呼ばれるコードを取り出す。

【0091】このMDは、HASH関数の性質から元のデータの内容が少しでも変わると大きく変化するという特徴がある。

【0092】次に、第3者から厳重に秘密を守られた暗号鍵を用いてMDを暗号化する。

【0093】この暗号化されたMDがMACであり、通信時にはデータと共にこのMACを通信相手に送信する。

【0094】受信した側では、まず、データから上述と同じようにデータに所定の演算を施してMDを得る。

【0095】次に、一緒に受信したMACから、復号化の鍵を用いて復号化してMD´を得る。

【0096】もし、通信途中でデータが改竄されるとMDとMD´とは異なるコードになるため、MDとMD´とを比較することで通信途中におけるデータの改竄の有無を調べることができる。

【0097】以上がMACによるデータの改竄検知の方法である。

【0098】因みに、MDを暗号化するときにデータ送信側と受信側で同じ暗号化／復号化鍵を用いる共通鍵暗号方式のアルゴリズムを用いたコードをMAC、データ送信側が秘密鍵でMDを暗号化し、受信側がそれを公開鍵で復号化した場合を一般に電子署名と呼ぶ場合もあるが、この発明では両者を総称してMACと呼ぶことにする。

【0099】（16）の発明では、データを（9）の発明による手法でユーザー領域に記録するときに、まず、MDを求める。

【0100】その後、このMDを図35に示すように（9）の発明のＦＡＴエントリ中にMD（ハッシュ値）を記録する。

【0101】通常、MACの場合には、MDを通信等の途中で改竄されないように暗号化する必要がある。

【0102】しかし、本発明では前提としてシステム管理領域全体が暗号化されるようになつている。

【0103】したがって、MDを、特に、暗号化しないでシステム管理領域にあるＦＡＴエントリに記録してもMACと同様の効果を得ることができる。

【0104】さらには、本発明では、改竄検知の処理をパスするモードを設けることで、上記（3）の発明と同じ処理速度でデータを読み出すことが可能になるという効果が得られる。

【0105】（17）の発明は、上記（16）の発明によって記録されたMD（ハッシュ値）を用いて改竄検知のための照合処理を行うもので、上記（3）の発明によるデータ再生装置に適用される。

【0106】また、本発明によると、上記課題を解決するために、（18） 前記システム管理用データ再生手段は、前記システム管理領域から前記パラメータを読み出すパラメータ読み出し手段と、前記システム管理領域から読み出したパラメータを用いて生成したランダムデータと、前記可搬型記録媒体の未使用領域のクラスタに記載されているランダムデータとを照合する手段と、を有することを特徴とする（3）記載のデータ再生装置が提供される。

【0107】この（18）の発明は後述する第2の実施の形態が対応し、関連する図は図20乃至図22である。

【0108】（作用効果）この（18）の発明は、上記（6），（7）の発明のデータ記録装置で記録されたデータを読み出すためのデータ再生装置である。

【0109】この（18）の発明によれば、悪意あるユーザーが他の記録装置を用いてデータを不正に消去した場合でも、消去されたユーザー領域のビットパターンが上記（6），（7）の発明によつて記録されたパターンと異なることから、不正にデータを消去したという痕跡を残すことができるという効果が得られる。

【0110】

【発明の実施の形態】以下図面を参照して本発明の実施の形態について説明する。

【0111】（第1の実施形態）まず、図1、図3、図4、図6乃至図10を用いて、本発明によるデータ記録／再生装置の第1の実施形態について説明する。

【0112】なお、これらの各図中で同じ番号が割り当てられた部分は、同じ機能を持つものとする。

【0113】図1は、第1の実施形態におけるデータ記憶／再生装置の構成を示すブロック図である。

【0114】すなわち、このデータ記憶／再生装置101は、外部のPC110と通信を行う通信部102と、この通信部102にそれぞれ内部バスを介して接続されている作業用メモリ部103、鍵データ記憶用メモリ部

104、制御部105、復号化部106、暗号化部107、可搬型記憶媒体駆動部108、媒体判定部109から構成される。

【0115】通信部102は、SCSI（Small Computer SystemInterface）やイーサネット、シリアルケーブル等の通信ケーブル、あるいは赤外線などの無線を用いて、データ記録／再生装置外部のPC110やワークステーションなどのデータ作成・編集装置とデータやコマンドのやり取りをする機能を持つ。

【0116】作業用メモリ103は、通信部102などから送られてきたデータや、各種処理の途中段階のデータをバッファリングすると共に、プログラムをロードするためのメモリである。

【0117】また、鍵データ格納用メモリ部104は、秘密情報、例えば、DES等の暗号鍵を格納するためのメモリである。

【0118】制御部105は、データ記憶／再生装置101の処理全体を制御する部分である。

【0119】復号化部106は、鍵データ格納用メモリ部104からデータを復号化するための情報を読み出し、データを復号化する。

【0120】同様に暗号化部107は、鍵データ格納用メモリ部104からデータを暗号化するための情報を読み出し、データを暗号化する。

【0121】また、可搬型記憶媒体駆動部108は、制御部105からの処理要求に応じ、当該データ記憶／再生装置101に装填される可搬型記憶媒体100上の領域のデータの読み出し／書き込み（消去を含む）を行う。

【0122】媒体判定部109は、当該データ記憶／再生装置101に装填される記憶媒体が、本発明による手法で記録されている可搬型記憶媒体100であるか、それ以外の記憶媒体であるかを判定する。

【0123】図3は、一般的なファイルシステムを説明するための図であり、ここではWindowsやMS-DOSで用いられているFATファイルシステムの記憶媒体1上の構成を示している。

【0124】一般に、FATファイルシステムの記憶媒体1では、システム管理領域7として、ブートセクタ（OEM IDやローダールーチン、デバイスに関する情報が記録されているBPB、及び予約領域からなる）2、FAT3、FATのコピー4、及びルートディレクトリのエントリテーブル5で構成されていると共に、ユーザー領域8としてファイル領域6で構成されている（詳細は次の文献を参照："MS-DOSエンサイクロペディアVolume1"、アスキー出版局（1989）p112-118）。

【0125】一方、図4は、本発明による第1の実施形態で用いられる可搬型記憶媒体100上の構成を示している。

【0126】図4では、システム管理領域7のデータは、図1の鍵データ格納用メモリ部104に格納されている暗号化鍵データと同じ鍵データで、且つ暗号化部107の暗号化法と同じ方法で暗号化されて記録されている。

【0127】図6は、本発明による第1の実施形態におけるデータ読み出し時の処理の流れを示すフローチャートである。

【0128】可搬型記憶媒体100からデータを読み出すときには、外部のPC110等からの可搬型記憶媒体100上のデータ読み出し要求（ステップS1）に応じて、まず、可搬型記憶媒体100のシステム管理領域に暗号化されて記録されているシステム管理用データを、可搬型記憶媒体駆動部108を用いて作業用メモリ103へ読み出す（ステップS2）。

【0129】その後、読み出した暗号化されているシステム管理用データを、復号化部106を用いて復号化し（ステップS3）、システム管理用のデータを得る。

【0130】システム管理用のデータが得られたならば、その情報を用いて指定のデータを読み出し（ステップS4）、通信部101を介して外部のPC110へ読み出したデータを送信して終了する（ステップS5）。

【0131】図7は、第1の実施形態で可搬型記憶媒体100へ初めてアクセスしてデータを読み出すときの処理の流れを示すフローチャートである。

【0132】可搬型記憶媒体100へ初めてアクセスしてデータを読み出すときには、外部のPC110等からの可搬型記憶媒体100上のデータ読み出し要求（ステップS21）に応じて、まず、アクセスが初めてであるか否かを判定（ステップS22）する。

【0133】そして、アクセスが初めてあるときには、可搬型記憶媒体100のシステム管理領域に暗号化されて記録されているシステム管理用データを、可搬型記憶媒体駆動部108を用いて作業用メモリ103へ読み出す（ステップS23）。

【0134】その後、読み出した暗号化されているシステム管理用データを、復号化部106を用いて復号化し（ステップS24）、システム管理用のデータを得る。

【0135】システム管理用のデータが得られたならば、その情報を用いて指定のデータを読み出し（ステップS25）、通信部102を介して外部のPC110へ読み出したデータを送信して終了する（ステップS26）。

【0136】しかるに、ステップS22において、アクセスが初めてではないときには、上記のステップS23，S24の処理をスルーして、前に得られているシステム管理用のデータの情報を用いて指定のデータを読み出し（ステップS25）、通信部102を介して外部のPC110へ読み出したデータを送信して終了する（ス

テップＳ２６）。

【０１３７】図８は、第１の実施形態でデータを書き込むときの処理の流れを示すフローチャートである。

【０１３８】通信部１０２を介して外部のＰＣ１００から受け取ったデータを可搬型記憶媒体１００へ書き込む場合には、まず、読み出し時と同様の手順で、システム管理用のデータを作業用メモリ１０３へ読み出す（ステップＳ４０、Ｓ４１）。

【０１３９】その後、復号化されたシステム管理用のデータを用いて、外部のＰＣ１００から受け取ったデータを可搬型記憶媒体１００へ書き込む（ステップＳ４２、Ｓ４３）。

【０１４０】このとき、可搬型記憶媒体１００上のデータの構成が更新されているので、当然、作業用メモリ１０３上のシステム管理用のデータも更新する（ステップＳ４４）。

【０１４１】その後、作業用メモリ１０３上のシステム管理用のデータを暗号化部１０７を用いて暗号化し（ステップＳ４５）、可搬型記憶媒体駆動部１０８を用いて上記暗号化したシステム管理用のデータを可搬型記憶媒体１００のシステム管理領域に書き込み（ステップＳ４６）、終了する（ステップＳ４７）。

【０１４２】図９は、第１の実施形態で可搬型記憶媒体１００へ初めてアクセスしてデータを書き込むときの処理の流れを示すフローチャートである。

【０１４３】可搬型記憶媒体１００へ初めてアクセスしてデータを書き込むときには、外部のＰＣ１１０等からの可搬型記憶媒体１００上のデータ書き込み要求（ステップＳ６０）に応じて、まず、アクセスが初めてであるか否かを判定（ステップＳ６１）する。

【０１４４】そして、アクセスが初めてあるときには、可搬型記憶媒体１００のシステム管理領域に暗号化されて記録されているシステム管理用データを、可搬型記憶媒体駆動部１０８を用いて作業用メモリ１０３へ読み出す（ステップＳ６２）。

【０１４５】その後、復号化されたシステム管理用のデータを用いて、外部のＰＣ１００から受け取ったデータを可搬型記憶媒体１００へ書き込む（ステップＳ６３、Ｓ６４）。

【０１４６】このとき、可搬型記憶媒体１００上のデータの構成が更新されているので、当然、作業用メモリ１０３上のシステム管理用のデータも更新する（ステップＳ６５）。

【０１４７】その後、作業用メモリ１０３上のシステム管理用のデータを暗号化部１０７を用いて暗号化し（ステップＳ６６）、可搬型記憶媒体駆動部１０８を用いて上記暗号化したシステム管理用のデータを可搬型記憶媒体１００のシステム管理領域に書き込み（ステップＳ６７）、終了する（ステップＳ６８）。

【０１４８】しかるに、ステップＳ６１において、アクセスが初めてではないときには、上記のステップＳ６２，Ｓ６３の処理をスルーして、前に得られているシステム管理用のデータの情報を用いて、外部のＰＣ１００から受け取ったデータを可搬型記憶媒体１００へ書き込む（ステップＳ６３、Ｓ６４）。

【０１４９】このとき、可搬型記憶媒体１００上のデータの構成が更新されているので、当然、作業用メモリ１０３上のシステム管理用のデータも更新する（ステップＳ６５）。

【０１５０】その後、作業用メモリ１０３上のシステム管理用のデータを暗号化部１０７を用いて暗号化し（ステップＳ６６）、可搬型記憶媒体駆動部１０８を用いて上記暗号化したシステム管理用のデータを可搬型記憶媒体１００のシステム管理領域に書き込み（ステップＳ６７）、終了する（ステップＳ６８）。

【０１５１】すなわち、システム管理用のデータは、毎回暗号化して可搬型記憶媒体１００のシステム管理領域に書き込まれることになる。

【０１５２】図１０の（ａ）は、第１の実施形態で可搬型記憶媒体１００へ初めてアクセスしてデータを書き込むときの処理の流れを示す他のフローチャートである。

【０１５３】可搬型記憶媒体１００へ初めてアクセスしてデータを書き込むときには、外部のＰＣ１１０等からの可搬型記憶媒体１００上のデータ書き込み要求（ステップＳ８０）に応じて、まず、アクセスが初めてであるか否かを判定（ステップＳ８１）する。

【０１５４】そして、アクセスが初めてあるときには、可搬型記憶媒体１００のシステム管理領域に暗号化されて記録されているシステム管理用データを、可搬型記憶媒体駆動部１０８を用いて作業用メモリ１０３へ読み出す（ステップＳ８２）。

【０１５５】その後、復号化されたシステム管理用のデータを用いて、外部のＰＣ１００から受け取ったデータを可搬型記憶媒体１００へ書き込む（ステップＳ８３、Ｓ８４）。

【０１５６】このとき、可搬型記憶媒体１００上のデータの構成が更新されているので、当然、作業用メモリ１０３上のシステム管理用のデータも更新して（ステップＳ８５）、終了する（ステップＳ８６）。

【０１５７】しかるに、ステップＳ８１において、アクセスが初めてではないときには、上記のステップＳ８２，Ｓ８３の処理をスルーして、前に得られているシステム管理用のデータの情報を用いて、外部のＰＣ１００から受け取ったデータを可搬型記憶媒体１００へ書き込む（ステップＳ８４）。

【０１５８】このとき、可搬型記憶媒体１００上のデータの構成が更新されているので、当然、作業用メモリ１０３上のシステム管理用のデータも更新して（ステップＳ８５）、終了する（ステップＳ８６）。

【０１５９】図１０の（ｂ）は、第１の実施形態で可搬

型記憶媒体１００の排出要求があったときの処理の流れを示すフローチャートである。

【０１６０】すなわち、可搬型記憶媒体１００の排出要求があったときには、システム管理用データを暗号化（ステップS９１）し、この暗号化されたシステム管理用のデータを可搬型記憶媒体１００上のシステム管理領域に記録（ステップS９２）した後、可搬型記憶媒体１００を排出する（ステップS９３）。

【０１６１】すなわち、可搬型記憶媒体１００を本発明によるデータ記録／再生装置１０１から排出するときだけ、システム管理用データを暗号化して可搬型記憶媒体１００上のシステム管理領域に記録するものである。

【０１６２】なお、以上の説明では、システム管理領域のデータを全て暗号化しているが、図５に示すように、ＦＡＴ、ＦＡＴのコピー、及びルートディレクトリのエントリテーブルのみを暗号化するようにしてもよい。

【０１６３】また、ここまでの説明ではデータ記録装置の外部装置としてＰＣを例に説明したが、外部の装置としては、これに限定されない。

【０１６４】例えば、ＰＣの代わりにワークステーション、ＰＤＡ等の情報編集機器であってもよいし、あるいはスキャナーやデジタルカメラ、デジタルビデオカメラのような映像撮像装置であっても構わない。

【０１６５】なお、この発明の実施の形態の各構成は、当然、各種の変形、変更が可能である。

【０１６６】図２に示すように、映像撮像装置１３０としては、光学系１２０、撮像部１２１、Ａ／Ｄ変換部１２２、画像処理部１２３、フォーマット変換部１２４、ユーザーインタフエイス部１２５から構成されるとともに、データ記録／再生装置１０１としての構成要素である作業用メモリ部１０３、鍵データ記憶用メモリ部１０４、制御部１０５、復号化部１０６、暗号化部１０７、可搬型記憶媒体駆動部１０８、媒体判定部１０９から構成される。

【０１６７】光学系１２０は、レンズ、鏡筒駆動系などから構成され、映像を撮像部１２１に結像する。

【０１６８】また、撮像部１２１は光信号を電気信号に変換し、Ａ／Ｄ変換部１２２では、前記電気信号をＡ／Ｄ変換してデジタル化したデータを作業用メモリ部１０３へ格納する。

【０１６９】画像処理部１２３では、前記の作業用メモリ１０３に格納されたデジタルデータから、画像を生成するための各種処理（例えば、ホワイトバランスの調整、ガンマ変換、エッヂ強調処理など）を施す。

【０１７０】フォーマット変換部１２４は、前記の画像のデータをＪＰＥＧ等の保存形式に変換する部分である。

【０１７１】また、ユーザーインタフェイス部１２５は、シャッター、液晶ファインダー、各種撮影モード設定用のボタンなどのユーザーインタフェイスからなる。

【０１７２】ファイルの消去などの要求もユーザーインタフェイス部１２５を介して入力される。

【０１７３】図２から分かるように、上記のような構成でも、図２の点線内は第１の実施形態のデータ記録／再生装置と同じである。

【０１７４】また、第１の実施形態の場合に、通信部１０２を通して外部のＰＣ１１０等とデータのやり取りをしていた部分が、図２では映像撮像装置内の点線外部との間でデータをやり取りすることに置き換わっただけである。

【０１７５】したがって、図２のような構成においても、第１の実施形態の機能を備えることが可能である。

【０１７６】上記のような構成によって、画像のような大容量のデータを、データ内容の秘匿性、真正性を確保し、且つ高速にデータを記録できるデータ記録装置を提供することが可能になる。

【０１７７】そして、上述したような第１の実施の形態には、以下のような発明が含まれている。

【０１７８】（１）　可搬型記憶媒体にデータを記録するデータ記録／再生装置において、装置内に秘密情報を保持する手段と、前記秘密情報を用いて暗号化及び復号化を行う手段と、前記暗号化手段を用いて、前記可搬型媒体のシステム管理用データ、もしくはシステム管理用データの一部を暗号化して前記可搬型記憶媒体のシステム管理領域へ記録する手段と、前記可搬型記憶媒体のシステム管理領域から、前記暗号化された前記システム管理用データを読み出し、前記復号化手段を用いて前記暗号化されたシステム管理用データ、もしくは暗号化されたシステム管理用データの一部を復号化する手段と、を有することを特徴とするデータ記録／再生装置。

【０１７９】（２）　前記データ記録／再生装置は、データを前記可搬型記憶媒体のユーザー領域へ書き込む処理を行っているときに、時間的に並行して前記暗号化の処理を行うことを特徴とするデータ記録／再生装置。

【０１８０】（第２の実施形態）ところで、上述したような第１の実施形態による手法においては、可搬型記録媒体上のデータをダンプして、順次読み出し位置を変えるという不正なアタック方法でデータ内容を読み出される可能性を有しているという危険がある。

【０１８１】特に、デジタルカメラで撮影した画像を格納するような記録媒体の場合、撮影するデータの種類（“ＷＯＲＤ”，“ｅｘｃｅｌ”，“ｔｅｘｔ”，“ｊｐｅｇ”“ｔｉｆｆ”，“ｍｐｅｇ”等のフォーマットのこと）も決まっており（ＪＰＥＧ，ＴＩＦＦ，ＦｌａｓｈＰｉｘ等）、さらにデータサイズもＣＣＤの画素数が固定であることによってほぼ一定であるので、第１の実施形態による手法においては、上述のような不正なアタックに対して弱いという難点がある。

【０１８２】そこで、この第２の実施形態では、このような不正なアタックに対する防御対策を伴ったデータ記

録／再生装置を提供することを意図している。
【0183】まず、この第2の実施形態で用いる用語について説明する。
【0184】
（1）論理的にアクセス可能な単位領域＝クラスタ
（2）物理的にアクセス可能な単位領域＝セクタ
（3）FAT　　：File Allocation Tableの略語であり、MS-DOSのファイルシステム名である。以下の説明の中では、FATをファイルシステムが用いる管理テーブルの総称のように用いているが、“FAT”というのは飽くまでMS-DOSやWindowsで用いられているファイルシステムで用いている管理テーブルの名称である。
（4）疑似欠陥クラスタ：実際に物理的に壊れているわけではなく、正常か欠陥かを示す管理テーブルの内容を操作することで欠陥としたクラスタ（本明細書内での定義）。
（5）疑似ランダム　　：疑似乱数系列を用いて乱数を生成するため、“疑似”という言葉が付く。
【0185】次に、第2の実施形態の概要について説明する。
【0186】この第2の実施形態では、システム管理領域（FATを含む）を暗号化することをベースに、大きく分けて以下の5つの手法が含まれている。
【0187】（1）データに対するクラスタの物理的な配置を疑似ランダム化する（連続性をなくす）。
【0188】（2）疑似欠陥クラスタを作り、データの読み出しを困難にする。
【0189】なお、上記（1），（2）に従属して以下のケースがある。
【0190】a）データ初期化時に、ユーザー領域を疑似ランダムデータで初期化する。
【0191】b）データ削除のときは、その領域を元のランダムデータに置き換える。
【0192】これは、未使用かつ初期化時と異なるデータが記録されたクラスタがあるときに改竄の疑いありとするためである。
【0193】（3）データ書き込み時にMOディスク等の記録媒体の未使用領域（上記疑似欠陥クラスタ領域も含む）に偽のデータも同時に書き込む。
【0194】なお、この（3）はについては、上記（1）、（2）と併用可能である。
【0195】（4）データに対する追記がない、データのサイズがほぼ一定であることを利用し、FATの小規模化（FAT暗号化の演算量を削減）を実現する。
【0196】なお、この（4）に従属して以下のケースがある。
【0197】a）データ記録時にシャッフルするなどの各種処理を行う。
【0198】b）処理のパラメータをシステム管理額域に記録する。
【0199】（5）データ記録時に、データのハッシュ値（OR Error Correcting Code／Error Detecting Code）を求め、システム管理領域に記録する。
【0200】図11は、以上のような概要に基づく第2の実施形態の上記の5つの手法に対応するMS-DOS FAT16ファイルシステムのファイル管理手法を説明するための図である。
【0201】すなわち、図11は、ファイル名file.textのファイルに対するアクセスを例にとったものである。
【0202】この場合、ルートディレクトリのエントリ（又は、サブディレクトリのエントリ）を検索することにより、図11中にメニュー形式で示すようなfile.textのディレクトリエントリ（FAT16）を探す。
【0203】ここでは、開始クラスタ（ID）としてFATエントリ（ID）が14である場合を示している。
【0204】なお、図11中にメニュー形式で示すようなファイルの大きさは、4800bytesであって、例えば、1クラスタ＝1024bytesであれば、5クラスタが必要となる場合を示している。
【0205】また、ここでは、1クラスタ＝2セクタ＝1024bytesである場合を示している。
【0206】図11中の“H”は、16進数を意味するものとする。
【0207】そして、FATエントリ（ID）が11，12，13，14，15，16，17，18，19，20に対して、各クラスタCH，DH，FFFFH，FH，10H，12H，FFF7H，13H，FFFFH，0Hがそれぞれ上記疑似ランダムによるランダム化されて割り当てられている例である。
【0208】この例では、1つのデータのFATリンク以下のようになる。
【0209】まず、開始クラスタ（ID）としてFATエントリ（ID）が14からアクセスが開始され、FH＝15でFATエントリ（ID）が15に移行し、10H＝16でFATエントリ（ID）が16に移行し、12H＝18でFATエントリ（ID）が18に移行し、13H＝19でFATエントリ（ID）が19に移行する。
【0210】なお、FATエントリ（ID）が17のFFF7Hは、上記疑似欠陥クラスタ領域としての不良クラスタであるため、FATエントリ（ID）が16からFATエントリ（ID）が18に移行している。
【0211】また、FATエントリ（ID）が19のFFF8～FFFFHは、ファイルの最後のクラスタである。
【0212】そして、FATエントリ（ID）が20の

０Ｈは、未使用クラスタである。

【０２１３】次に、以上のような概要に基づく第２の実施形態の上記の５つの手法に対応する各具体例について図１２乃至図３７を参照して説明する。

【０２１４】なお、これらの各図中で上述した第１の実施形態と同じ番号が割り当てられた部分は、同じ機能を持つものとする。

【０２１５】（第１の具体例）まず、図１２乃至図１７を用いて、本発明によるデータ記録／再生装置の第２の実施形態の第１の具体例について説明する。

【０２１６】図１２は、第２の実施形態における第１の具体例によるデータ記録／再生装置の構成を示すブロック図である。

【０２１７】すなわち、このデータ記憶／再生装置１０１は、外部のＰＣ１１０と通信を行う通信部１０２と、この通信部１０２にそれぞれ内部バスを介して接続されている作業用メモリ部１０３、鍵データ記憶用メモリ部１０４、制御部１０５、復号化部１０６、暗号化部１０７、可搬型記憶媒体駆動部１０８、媒体判定部１０９（図示せず、第１の実施形態参照）、データ分割部２０１、クラスタ選択部２０２から構成される。

【０２１８】通信部１０２は、ＳＣＳＩ（Ｓｍａｌｌ Ｃｏｍｐｕｔｅｒ ＳｙｓｔｅｍＩｎｔｅｒｆａｃｅ）やイーサネット、シリアルケーブル等の通信ケーブル、あるいは赤外線などの無線を用いて、データ記録／再生装置外部のＰＣ１１０やワークステーションなどのデータ作成・編集装置とデータやコマンドのやり取りをする機能を持つ。

【０２１９】作業用メモリ１０３は、通信部１０２などから送られてきたデータや、各種処理の途中段階のデータをバッファリングすると共に、プログラムをロードするためのメモリである。

【０２２０】また、鍵データ格納用メモリ部１０４は、秘密情報、例えば、ＤＥＳ等の暗号鍵を格納するためのメモリである。

【０２２１】制御部１０５は、データ記憶／再生装置１０１の処理全体を制御する部分である。

【０２２２】復号化部１０６は、鍵データ格納用メモリ部１０４からデータを復号化するための情報を読み出し、データを復号化する。

【０２２３】同様に暗号化部１０７は、鍵データ格納用メモリ部１０４からデータを暗号化するための情報を読み出し、データを暗号化する。

【０２２４】また、可搬型記憶媒体駆動部１０８は、制御部１０５からの処理要求に応じ、当該データ記憶／再生装置１０１に装填される可搬型記憶媒体１００上の領域のデータの読み出し／書き込み（消去を含む）を行う。

【０２２５】なお、図示しない媒体判定部１０９では、当該データ記憶／再生装置１０１に装填される記憶媒体が、本発明による手法で記録されている可搬型記憶媒体１００であるか、それ以外の記憶媒体であるかを判定する。

【０２２６】データ分割部２０１は、データを可搬型記録媒体１００上で論理的にアクセス可能な単位領域のサイズに分割する。

【０２２７】クラスタ選択部２０２は、所定の規則に従って可搬型記録媒体１００から使用されていないクラスタを論理的にアクセス可能な単位領域のクラスタとして選択する。

【０２２８】すなわち、この第１の具体例によるデータ記録／再生装置は、上述したような第１の実施形態によるデータ記録／再生装置において、データを可搬型記録媒体１００に記録する処理において、データ分割部２０１によりデータを可搬型記録媒体１００上で論理的にアクセス可能な単位領域のサイズに分割すると共に、クラスタ選択部２０２により所定の規則に従って可搬型記録媒体１００から使用されていないクラスタを論理的にアクセス可能な単位領域のクラスタとして選択することにより、制御部１０５からの処理要求に応じて前記分割されたデータを前記選択された論理的にアクセス可能な単位領域のクラスタに逐次記録することを特徴としている。

【０２２９】すなわち、通常、データを可搬型記録媒体としての例えばＭＯ等のディスクに記録するときには、クラスタが連続的につながっている領域にデータを記録するようにしているが、この方法だと、ディスクのユーザー領域を順次ダンプしていくことで、ディスクに書き込まれたデータが読み出されるという脅威がある。

【０２３０】そこで、この第１の具体例によるデータ記録／再生装置では、データを書き込むときに、あえて連続性のないクラスタを選んでデータを書き込むことで、上記脅威を回避する手法を採用するものとしている。

【０２３１】例えば、ディスクサイズ１Ｇ、画像サイズ６Ｍ（２００万画素非圧縮）の場合、クラスタのサイズが１６Ｋのケースでも、ディスク全体のクラスタ数は６２５００個あり、画像データ１つを記録するためのクラスタ数は３７５個ある。

【０２３２】このようなディスクに対して第１の具体例による手法を採用すれば、システム管理領域が暗号化されてクラスタ間のリンクが分からない場合には、手探りで画像データを復元しようにも、６２５００個のクラスタから（初期化時にディス．クの全領域にランダムなデータを書き込んでいるので）正しい順番で３７５個のクラスタに記録されたデータを読みださなければならず、解読は相当困難になる（単純計算で約62500^{375}通りの組み合わせがある）。

【０２３３】仮に、データを書き込む前と後の記録媒体全領域がダンプされ、前記２つのダンプされたデータ比較することにより、データが記録されている領域があば

かれたとしても、データを読み出すためのデータの順番がわからないので、375！通りの組み合わせから本当のデータを解読する必要がある。

【0234】実際には、画像データの場合、周波数や色相関などの情報から、375！通りよりもう少し探索範囲を狭めることは可能ではあるが、解読自体は不可能に近いと言える。

【0235】そして、この第1の具体例による手法では、クラスタの物理的な連続性がなくなるため、読み出し速度は低下するが、基本的に通常のファイルステムと同じで、システム管理領域のデータサイズは変わらない。

【0236】図13は、この第1の具体例による手法に基づいたFAT16ファイルシステムにおけるデータ管理形態を示している。

【0237】すなわち、図13は、先に第2の実施形態の概要について説明した図11からクラスタ部分を取り出して示したものであって、疑似欠陥クラスタ領域を設けていない以外は図11に準じている。

【0238】この例では、1つのデータのFATリンク以下のようになる。

【0239】まず、開始クラスタ(ID)としてFATエントリ(ID)が14からアクセスが開始され、FH=15でFATエントリ(ID)が15に移行し、10H=16でFATエントリ(ID)が16に移行し、11H=17でFATエントリ(ID)が17に移行し、12H=18でFATエントリ(ID)が18に移行する。

【0240】なお、FATエントリ(ID)が18のFFFHは、ファイルの最後のクラスタである。

【0241】図14は、通常のファイルシステムを用いた場合に、システム管理領域とユーザー領域とを有する可搬型記録媒体のユーザー領域にデータが記録されるときの例を参考的に示している。

【0242】この場合、可搬型記録媒体では、データの物理的配置として、例えば、ID(アドレス)=2～37のクラスタ領域をできるだけ物理的な連続性を確保するように配置されている。

【0243】そして、この図14においては、ハッチングを有するID(アドレス)=14～18のクラスタ領域にデータが書き込まれる例を示している。

【0244】図15は、この第1の具体例による手法に基づいたデータの記録形態を示している。

【0245】すなわち、この図15においては、記録するデータは、まず、クラスタのサイズに分割され、各々、ランダムに選択されたクラスタID(アドレス)=2，3，4…12，13，14…17，18，19…33のクラスタ領域に記録されることを示している。

【0246】図16は、この第1の具体例による場合の1つのデータのFATリンクを図14の一部と対応付けて示している。

【0247】この図16から分かるように、基本的にFATシステムで扱うことが可能な手法である。

【0248】図17は、この第1の具体例によるファイルシステムを用いた場合に、システム管理領域とユーザー領域とを有する可搬型記録媒体のユーザー領域にデータが記録されるときの例を示している。

【0249】この場合、可搬型記録媒体では、データの物理的配置として、例えば、ID(アドレス)=2～37のクラスタ領域をできるだけ物理的な連続性をなくすようにランダム化して配置されている。

【0250】そして、この図17においては、ハッチングを有するID(アドレス)=3，12，14，17，19，33クラスタ領域にデータが書き込まれる例を示している。

【0251】(第2の具体例)次に、図18及び図19を用いて、本発明によるデータ記録／再生装置の第2の実施形態の第2の具体例について説明する。

【0252】図18は、第2の実施形態における第2の具体例によるデータ記録／再生装置の構成を示すブロック図である。

【0253】すなわち、このデータ記憶／再生装置101は、外部のPC110と通信を行う通信部102と、この通信部102にそれぞれ内部バスを介して接続されている作業用メモリ部103、鍵データ記憶用メモリ部104、制御部105、復号化部106、暗号化部107、可搬型記憶媒体駆動部108、媒体判定部109(図示せず、第1の実施形態参照)、クラスタ選択部301、乱数発生部302から構成される。

【0254】通信部102は、SCSI(Small Computer SystemInterface)やイーサネット、シリアルケーブル等の通信ケーブル、あるいは赤外線などの無線を用いて、データ記録／再生装置外部のPC110やワークステーションなどのデータ作成・編集装置とデータやコマンドのやり取りをする機能を持つ。

【0255】作業用メモリ103は、通信部102などから送られてきたデータや、各種処理の途中段階のデータをバッファリングすると共に、プログラムをロードするためのメモリである。

【0256】また、鍵データ格納用メモリ部104は、秘密情報、例えば、DES等の暗号鍵を格納するためのメモリである。

【0257】制御部105は、データ記憶／再生装置101の処理全体を制御する部分であり、後述する欠陥クラスタ情報の書き込み制御はこの制御部105で行われることになる。

【0258】復号化部106は、鍵データ格納用メモリ部104からデータを復号化するための情報を読み出し、データを復号化する。

【０２５９】同様に暗号化部１０７は、鍵データ格納用メモリ部１０４からデータを暗号化するための情報を読み出し、データを暗号化する。

【０２６０】また、可搬型記憶媒体駆動部１０８は、制御部１０５からの処理要求に応じ、当該データ記憶／再生装置１０１に装填される可搬型記憶媒体１００上の領域のデータの読み出し／書き込み（消去を含む）を行う。

【０２６１】なお、図示しない媒体判定部１０９では、当該データ記憶／再生装置１０１に装填される記憶媒体が、本発明による手法で記録されている可搬型記憶媒体１００であるか、それ以外の記憶媒体であるかを判定する。

【０２６２】クラスタ選択部３０１は、所定の規則に従って可搬型記録媒体１００から論理的にアクセス可能な単位領域のクラスタとして選択する。

【０２６３】乱数発生部３０２は、後述する欠陥クラスタ情報の書き込み制御に用いられるランダムなデータとして任意性のあるパラメータを用いたランダムデータを生成するための乱数を発生する。

【０２６４】すなわち、この第２の具体例によるデータ記録／再生装置は、上述したような第１の実施形態によるデータ記録／再生装置において、データを可搬型記録媒体１００に記録する処理において、クラスタ選択部３０１及び乱数発生部３０２とにより前記可搬型記録媒体１００から論理的にアクセス可能な単位領域をランダムに複数選ぶと共に、制御部１０５により前記可搬型記録媒体１００上で論理的にアクセス可能な単位領域を欠陥領域として前記システム管理用データに登録することを特徴としている。

【０２６５】そして、この第２の具体例では、初期化時に、可搬型記録媒体１００上にランダムに疑似欠陥クラスタを作ることを特徴としている。

【０２６６】ここでいう疑似欠陥クラスタとは、実際にユーザー領域のクラスタを破壊するのではなく、単に、ＦＡＴエントリに対応するクラスタが壊れているという情報を記録するだけである（システム管理用データを暗号化しているので、この情報は誰にも分からない）。

【０２６７】記録媒体に書き込まれるデータは、真のデータの所々に疑似欠陥セクタが入り込んでいる。

【０２６８】例えば、全クラスタの１０％が疑似欠陥セクタの場合、前例の条件では（３７５＋３８）個のクラスタに３８個の疑似欠陥クラスタ（偽データ）が含まれていることになる。

【０２６９】従って、データを読み出すためには６２５００個のクラスタ全体から、データが記録されている領域を探し出し、その後、さらに疑似欠陥クラスタの部分を取り除く必要がある。

【０２７０】仮に、データを書き込む前と後の記録媒体全領域がダンプされ、前記２つのダンプされたデータ比較することにより、データが記録されている領域があばかれたとしても、後述する第６乃至第１１の具体例による手法と併用することにより、データ内容を強靭に保護することが可能である。

【０２７１】なお、ＪＰＥＧ等の圧縮画像の場合には、各クラスタに記録されているデータそのものが直接画像を表現しないため、第６乃至第１１の具体例による手法と併用することは特に必要なく、この第２の具体例による手法のみでデータ内容を強靭に保護することが可能である。

【０２７２】この第２の具体例による手法では、疑似欠陥クラスタの分だけディスク領域に無駄が生じることになる。

【０２７３】しかし、この第２の具体例の場合、欠陥クラスタ情報は通常の方法で図１１に示したようにＦＡＴエントリ内に記録されるため、わざわざ欠陥クラスタ情報（位置）をＦＡＴ以外のところに別途記録しておく必要はない。

【０２７４】そして、この第２の具体例による手法では、基本的に通常のファイルステムと同じであるため実装が簡単であると共に、データを書き込むクラスタに連続性があるためデータの書き込み速度が速いという利点がある。

【０２７５】図１９の（ａ），（ｂ）は、通常の場合のＦＡＴリンクの初期化状態と、この第２の具体例による手法に基づいたＦＡＴリンクの初期化状態とを対比させて示している。

【０２７６】すなわち、図１９の（ａ）に示すように、通常の場合のＦＡＴリンクの初期化状態では、通常の場合と何等変わりがない。

【０２７７】これに対し、図１９の（ｂ）に示すように、この第２の具体例による手法では、ＦＡＴエントリ（ＩＤ）＝１２，１７のところに、ＦＦＦ７Ｈなる疑似欠陥クラスタ領域であることを示すコードが付されている。

【０２７８】（第３の具体例）次に、図２０乃至図２２を用いて、本発明によるデータ記録／再生装置の第２の実施形態の第３の具体例について説明する。

【０２７９】図２０は、第２の実施形態における第３の具体例によるデータ記録／再生装置の構成を示すブロック図である。

【０２８０】すなわち、このデータ記憶／再生装置１０１は、外部のＰＣ１１０と通信を行う通信部１０２と、この通信部１０２にそれぞれ内部バスを介して接続されている作業用メモリ部１０３、鍵データ記憶用メモリ部１０４、制御部１０５、復号化部１０６、暗号化部１０７、可搬型記憶媒体駆動部１０８、媒体判定部１０９（図示せず、第１の実施形態参照）、クラスタ照合部４０１、乱数発生部４０２から構成される。

【０２８１】通信部１０２は、ＳＣＳＩ（Ｓｍａｌｌ

Computer SystemInterface)やイーサネット、シリアルケーブル等の通信ケーブル、あるいは赤外線などの無線を用いて、データ記録／再生装置外部のPC110やワークステーションなどのデータ作成・編集装置とデータやコマンドのやり取りをする機能を持つ。

【0282】作業用メモリ103は、通信部102などから送られてきたデータや、各種処理の途中段階のデータをバッファリングすると共に、プログラムをロードするためのメモリである。

【0283】また、鍵データ格納用メモリ部104は、秘密情報、例えば、DES等の暗号鍵を格納するためのメモリである。

【0284】制御部105は、データ記憶／再生装置101の処理全体を制御する部分である。

【0285】復号化部106は、鍵データ格納用メモリ部104からデータを復号化するための情報を読み出し、データを復号化する。

【0286】同様に暗号化部107は、鍵データ格納用メモリ部104からデータを暗号化するための情報を読み出し、データを暗号化する。

【0287】また、可搬型記憶媒体駆動部108は、制御部105からの処理要求に応じ、当該データ記憶／再生装置101に装填される可搬型記憶媒体100上の領域のデータの読み出し／書き込み（消去を含む）を行う。

【0288】なお、図示しない媒体判定部109では、当該データ記憶／再生装置101に装填される記憶媒体が、本発明による手法で記録されている可搬型記憶媒体100であるか、それ以外の記憶媒体であるかを判定する。

【0289】クラスタ照合部401は、後述するように、システム管理領域から読み出したパラメータを用いて生成したランダムデータと、前記可搬型記録媒体の未使用領域のクラスタに記録されているデータとが初期化時と同じであるか否かを照合する。

【0290】乱数発生部402は、後述するユーザー領域全体に前記ランダムデータの書き込み制御に用いられるランダムなデータとして任意性のあるパラメータを用いたランダムデータを生成するための乱数を発生する。

【0291】すなわち、この第3の具体例によるデータ記録／再生装置は、上述したような第1の実施形態によるデータ記録／再生装置において、データを可搬型記録媒体100に記録する処理において、前記可搬型記録媒体を初期化するために、乱数発生部402により任意性のあるパラメータを用いてランダムなデータを生成して、制御部105からの処理要求に応じてユーザー領域全体に前記ランダムデータを書き込むと共に、前記システム管理領域に予め記録しておいた前記パラメータを読み出し、クラスタ照合部401により前記システム管理領域から読み出したパラメータを用いて生成したランダムデータと、前記可搬型記録媒体の未使用領域のクラスタに記録されているデータとが初期化時と同じであるか否かを照合し、制御部105からの処理要求に応じて前記可搬型記録媒体からデータを削除するときに、前記可搬型記録媒体の未使用の領域に疑似ランダムデータを書き込むことを特徴としている。

【0292】そして、この第3の具体例による手法は、前述した第1及び第2の具体例による手法を補うものである。

【0293】すなわち、通常、データを可搬型記録媒体としての例えばMO等のディスクに記録するときに、データが記録されていないディスクはディスク領域全体が例えば0（OFF）で初期化されている場合が考えられる。

【0294】そのような場合、前述した第1及び第2の具体例による手法だけではデータが記録されている領域とされていない領域は、ディスク全体をダンプすることですぐに分かってしまうという脅威がある。

【0295】そこで、この第3の具体例による手法では、予めディスク全体をランダムな値で初期化してしまうことにより、上記脅威を低減させる手法である。

【0296】この手法は、データを記録した後でデータ内容を改竄するアタックに対しては効果がある。

【0297】しかるに、この第3の具体例による手法では、データ記録前と記録後の差分をとるというアタックには何ら効果がないが、このアタックに対する対策は次に述べる第4の具体例による手法で対策することができる。

【0298】また、ファイルシステムに関する知識を有し、かつ悪意あるユーザーによって上記の初期化されたディスクのユーザー領域が他のデータ記録装置で低レベルの手段を用いて0などに一様に初期化される恐れがある。

【0299】そこで、この第3の具体例による手法では、未使用の領域には場所に依存する特定のデータ（疑似ランダムデータ）を書き込み、ユーザー領域に不正にデータが書き込まれていないかをチェックすることができる機能を備える。

【0300】このため、第3の具体例による手法では、具体的には、疑似乱数生成系列とその種（ここでは、パラメータと呼び、システム管理領域に暗号化して記録されるもの）を用いる。

【0301】すなわち、乱数生成の種が分かっていれば、どのクラスタにどんな乱数列が記録されたか分かるため、上記のようにユーザー領域に不正にデータが書き込まれていないかをチェックすることができるからである。

【0302】また、通常、データファイルを消去する場合には、単に、FATエントリから対応するFATリン

ク部分を未使用（0H）にするだけであるが、このようにすると上記の手法を採用することができない。

【0303】そこで、この第3の具体例による手法では、消去した場合には、そのファイルが使用していたクラスタの値を、上記乱数の種を用いて、初期化時と同じ値にするようにしている。

【0304】図21は、この第3の具体例による手法を説明するための概念図である。

【0305】図22は、この第3の具体例による手法を説明するためのフローチャートである。

【0306】すなわち、FATエントリのIDをnとし、システム管理領域に予め記録しておく前記パラメータをxとするとき、これらのn，xをランダムデータ生成装置に入力して1クラスタ分のランダムデータを生成する（ステップS11，S12，S13）。

【0307】そして、この1クラスタ分のランダムデータを可搬型記録媒体のユーザー領域におけるn番目のクラスタに記録するようにすることにより、ユーザー領域をランダムな値で全面的に初期化すると共に、システム管理用データを暗号化して可搬型記録媒体のシステム管理領域に記録した後、終了する（ステップS14，S15，S16，S17）。

【0308】（第4の具体例）次に、図23を用いて、本発明によるデータ記録／再生装置の第2の実施形態の第4の具体例について説明する。

【0309】図23は、第2の実施形態における第4の具体例によるデータ記録／再生装置の機能を説明するためのフローチャートである。

【0310】なお、この第4の具体例によるデータ記録／再生装置の構成については、前述した第3の具体例によるデータ記録／再生装置の構成と同じであるため、その説明を省略するものとする。

【0311】すなわち、この第4の具体例によるデータ記録／再生装置は、上述したような第1の実施形態によるデータ記録／再生装置において、データを可搬型記録媒体100に記録する処理において、乱数発生部402により任意性のあるパラメータを用いてランダムなデータを生成して、制御部105からの処理要求に応じてユーザー領域から複数選択した未使用の領域に前記ランダムなデータを書き込むことを特徴としている。

【0312】そして、この第4の具体例は、図23に示すように、ディスクにデータを記録するとき（ステップS51，S52）に、ダミーデータを同時に記録する（ステップS53～S57）という手法である。

【0313】すなわち、ダミーデータの同時記録については、FATエントリのIDをnとするとき、このnをランダムデータ生成装置に入力してランダムデータを生成する（ステップS53，S54）。

【0314】そして、未使用のクラスタ領域をランダムに選択し、この選択したクラスタ領域にランダムデータをN≦n（但し、Nは、ランダムデータを書き込むクラスタ領域数）となるまで記録するようにすると共に、システム管理用データを暗号化して可搬型記録媒体のシステム管理領域に記録した後、終了する（ステップS55，S56，S57，S58，S59）。

【0315】この第4の具体例による手法では、システム管理データが第1の実施形態に示したように暗号化されているので、ダミーデータが真のデータと一緒に記録されていることについては、ユーザーからは見分けがつかない。

【0316】また、ダミーデータは未使用領域（疑似欠陥クラスタを含む）を未使用のステータスのままで使うので、ディスク等の可搬型記録媒体領域をまったく無駄にしない（FATには一切記録しないので、ファイルにならない）。

【0317】（第5の具体例）次に、図24及び図25を用いて、本発明によるデータ記録／再生装置の第2の実施形態の第5の具体例について説明する。

【0318】図24は、第2の実施形態における第5の具体例によるデータ記録／再生装置の機能を説明するためにFATエントリ構成を示している図である。

【0319】このFATエントリ（ID）構成は、図24に示すように、開始クラスタID、最後のクラスタID、欠陥クラスタの個数、欠陥クラスタ1のID、欠陥クラスタ2のID等を有している。

【0320】図25の（a），（b）は、第1の具体例に準じた場合のFATファイルシステムと、この第5の具体例による手法に基づいたファイルシステムとを対比させて示している図である。

【0321】すなわち、図25の（a）に示すように、第1の具体例に準じた場合のFATファイルシステムでは、第1の具体例の場合とほぼ変わりがない。

【0322】これに対し、図25の（b）に示すように、この第2の具体例による手法では、FATエントリ（ID）＝K－1，K，K＋1，K＋2，K＋3，K＋4，K＋5において、開始クラスタ（ID）としてFATエントリ（ID）がK（14）からアクセスが開始され、K＋1（15），K＋2（1），K＋3（17）に移行する。

【0323】なお、この第5の具体例によるデータ記録／再生装置の構成については、前述した第2の具体例によるデータ記録／再生装置の構成と同じであるため、その説明を省略するものとする。

【0324】すなわち、この第5の具体例によるデータ記録／再生装置は、上述したような第1の実施形態によるデータ記録／再生装置において、データを可搬型記録媒体100に記録する処理において、前記システム管理領域に、データを記録する領域の、論理的にアクセス可能な先頭及び最後尾の単位領域のIDと、前記データを記録する連続領域内の欠陥領域の情報をファイル管理用

テーブルに記録すると共に、前記可搬型記録媒体上のデータに対する読み出し、書き込み等のアクセスを行う場合に、前記ファイル管理用テーブルからデータの可搬型記録媒体上の物理的なアドレスを求めることを特徴としている。

【0325】そして、この第5の具体例による手法は、以下に示すような観点に基づいている。

【0326】例えば、デジタルカメラのデータ記録装置の場合、200万画素の非圧縮データならば、そのデータのサイズは6Mバイトであり、FAT16のシステムでは必要なクラスタ数は、クラスタサイズを16Kバイトとしても367個となり、1つの画像ファイルを管理するのに必要な管理データは367×2=734バイト必要になる。

【0327】ところで、デジタルカメラでは、通常データに対して後から追記するような処理は行われないと共に、1つのデータは通常連続するクラスタに連続して記録される。

【0328】従って、通常のFATシステムの場合のようにFATの全てをリンクする必要はなく、クラスタの開始ID(アドレス)と最後のID及び、途中に欠陥クラスタがある場合にはその情報が記録されていれば、データにアクセスすることが可能である。

【0329】最近のMO等のディスクでは、欠陥クラスタがほとんど存在しないのが普通であるため、上記の手法でデータファイルを管理するのに必要な領域は、上記の例の場合、FAT16システムの数百分の1になる。

【0330】本システムでは、システム管理領域を暗号化することを考えると、システム管理領域のデータ量の削減は処理時間の短縮には極めて有効な手段であると考えられる。

【0331】この第5の具体例による手法は、連続するクラスタを用いることが条件であるため、上述した第1、第3及び第4の具体例による手法に対しては適用することができない。

【0332】(第6乃至第11の具体例)次に、図26乃至及び図32を用いて、本発明によるデータ記録/再生装置の第2の実施形態の第6乃至第11の具体例について説明する。

【0333】なお、この第6乃至第11の具体例は、いずれも前述した第5の具体例による手法に従属的に適用されるものである。

【0334】すなわち、この第6乃至第11の具体例は、前述した第5の具体例による手法が、データファイルを管理するのに必要なファイルシステムのデータ量を少なくできることを利用し、ファイルシステムのデータに書き込むデータをファイルに異なるでシャッフルしたり、暗号化したりできるようにする手法である。

【0335】図26は、第2の実施形態における第6乃至第11の具体例によるデータ記録/再生装置の機能を共通に説明するためにFATエントリ構成を示している図である。

【0336】このFATエントリ(ID)構成は、図26に示すように、開始クラスタID、最後のクラスタID、処理情報、欠陥クラスタの個数、欠陥クラスタ1のID、欠陥クラスタ2のID等を有している。

【0337】図27は、第2の実施形態における第6乃至第11の具体例によるデータ記録/再生装置の機能を共通に説明するためのフローチャートである。

【0338】この処理フローは、図27に示すように、まず、データが入力されると、データ処理情報を作成してFAT中に記録する(ステップS71, S72)。

【0339】次に、データ処理情報に従って入力データを処理すると共に、可搬型記憶媒体上にデータを記録する(ステップS73, S74)。

【0340】次に、FAT及びディレクトリエントリの情報を更新すると共に、システム管理用データを暗号化して可搬型記憶媒体上にデータを記録した後、終了する(ステップS75, S76, S77)。

【0341】そして、第6の具体例によるデータ記録/再生装置は、上述したような第5の具体例によるデータ記録/再生装置において、データを前記可搬型記憶媒体のユーザー領域へ書き込む処理を行うときに、データ全体、もしくはデータの一部に対して所定の処理を施すと共に、前記処理を施した領域のデータ上のアドレス、またはアドレスに関連する情報、及び前記処理に必要なパラメータをシステム管理用データに記録することを特徴としている。

【0342】図28は、第2の実施形態における第7の具体例によるデータ記録/再生装置の構成を示すブロック図である。

【0343】すなわち、このデータ記憶/再生装置101は、外部のPC110と通信を行う通信部102と、この通信部102にそれぞれ内部バスを介して接続されている作業用メモリ部103、鍵データ記憶用メモリ部104、制御部105、復号化部106、暗号化部107、可搬型記憶媒体駆動部108、媒体判定部109(図示せず、第1の実施形態参照)、シャッフル処理部501から構成されている。

【0344】通信部102は、SCSI(Small Computer SystemInterface)やイーサネット、シリアルケーブル等の通信ケーブル、あるいは赤外線などの無線を用いて、データ記録/再生装置外部のPC110やワークステーションなどのデータ作成・編集装置とデータやコマンドのやり取りをする機能を持つ。

【0345】作業用メモリ103は、通信部102などから送られてきたデータや、各種処理の途中段階のデータをバッファリングすると共に、プログラムをロードするためのメモリである。

【0346】また、鍵データ格納用メモリ部104は、秘密情報、例えば、DES等の暗号鍵を格納するためのメモリである。

【0347】制御部105は、データ記憶/再生装置101の処理全体を制御する部分である。

【0348】復号化部106は、鍵データ格納用メモリ部104からデータを復号化するための情報を読み出し、データを復号化する。

【0349】同様に暗号化部107は、鍵データ格納用メモリ部104からデータを暗号化するための情報を読み出し、データを暗号化する。

【0350】また、可搬型記憶媒体駆動部108は、制御部105からの処理要求に応じ、当該データ記憶/再生装置101に装填される可搬型記憶媒体100上の領域のデータの読み出し/書き込み(消去を含む)を行う。

【0351】なお、図示しない媒体判定部109では、当該データ記憶/再生装置101に装填される記憶媒体が、本発明による手法で記録されている可搬型記憶媒体100であるか、それ以外の記憶媒体であるかを判定する。

【0352】シャッフル処理部501は、上述したような第6の具体例によるデータ記録/再生装置において、前記所定の処理として、ブロック内のシャッフル処理を行うものである。

【0353】そして、この第7の具体例によるデータ記録/再生装置は、上述したような第6の具体例によるデータ記録/再生装置において、前記所定の処理として、を行うことを特徴としている。

【0354】図29は、第2の実施形態における第7の具体例によるデータ記録/再生装置の機能を説明するために示している図である。

【0355】すなわち、この第7の具体例による手法では、可搬型記憶媒体100上のユーザー領域のファイルfile.textのデータが記録されている領域で、クラスタ単位でシャッフル処理を行うと共に、その処理情報をシャッフル処理の情報(パラメータ等)を可搬型記憶媒体100上のシステム管理領域に記録するようにしている。

【0356】図30は、第2の実施形態における第8の具体例によるデータ記録/再生装置の機能を説明するために示している図である。

【0357】すなわち、この第8の具体例による手法では、前述した第7の具体例による手法と同様にシャッフル処理を行うものであるが、その際可搬型記憶媒体100上のユーザー領域のファイルfile.textのデータが記録されている領域で、クラスタ内でブロック単位でシャッフル処理を行うと共に、その処理情報をシャッフル処理の情報(パラメータ等)を可搬型記憶媒体100上のシステム管理領域に記録するようにしている。

【0358】そして、この第8の具体例によるデータ記録/再生装置は、上述したような第6の具体例によるデータ記録/再生装置において、前記所定の処理として、ブロック単位でシャッフル処理を行うことを特徴としている。

【0359】図31は、第2の実施形態における第9の具体例によるデータ記録/再生装置の機能を説明するために示している図である。

【0360】すなわち、この第9の具体例による手法では、前述した第7の具体例による手法と同様にシャッフル処理を行うものであるが、その際可搬型記憶媒体100上のユーザー領域のファイルfile.textのデータが記録されている領域で、データ全体に対してシャッフル処理を行うと共に、その処理情報をシャッフル処理の情報(パラメータ等)を可搬型記憶媒体100上のシステム管理領域に記録するようにしている。

【0361】そして、この第9の具体例によるデータ記録/再生装置は、上述したような第6の具体例によるデータ記録/再生装置において、前記所定の処理として、データ全体に対するシャッフル処理を行うことを特徴としている。

【0362】図32は、第2の実施形態における第10の具体例によるデータ記録/再生装置の機能を説明するために示している図である。

【0363】すなわち、この第10の具体例による手法では、前述した第7の具体例による手法のようにシャッフル処理を行うのでなく、可搬型記憶媒体100上のユーザー領域のファイルfile.textのデータが記録されている領域で、データ全体に対して暗号化処理を行うと共に、その処理情報をアルゴリズムに関する情報(暗号鍵の情報等)として可搬型記憶媒体100上のシステム管理領域に記録するようにしている。

【0364】そして、この第10の具体例によるデータ記録/再生装置は、上述したような第6の具体例によるデータ記録/再生装置において、前記所定の処理として、データ全体に対する暗号化処理を行うことを特徴としている。

【0365】そして、第11の具体例によるデータ記録/再生装置は、上述したような第7乃至第10の具体例によるデータ記録/再生装置において、前記所定の処理として、前記ブロック内のシャッフル処理、ブロック単位でシャッフル処理、データ全体に対するシャッフル処理及びデータ全体に対する暗号化処理のうちの少なくとも2つ以上の処理を組み合わせたことを特徴としている。

【0366】(第12の具体例)次に、図33乃至図38を用いて、本発明によるデータ記録/再生装置の第2の実施形態の第12の具体例について説明する。

【0367】図33は、第2の実施形態における第12の具体例によるデータ記録/再生装置の構成を示すブロ

ック図である。

【0368】すなわち、このデータ記憶／再生装置101は、外部のPC110と通信を行う通信部102と、この通信部102にそれぞれ内部バスを介して接続されている作業用メモリ部103、鍵データ記憶用メモリ部104、制御部105、復号化部106、暗号化部107、可搬型記憶媒体駆動部108、媒体判定部109（図示せず、第1の実施形態参照）、ハッシュ演算部601から構成される。

【0369】通信部102は、SCSI（Small Computer SystemInterface）やイーサネット、シリアルケーブル等の通信ケーブル、あるいは赤外線などの無線を用いて、データ記録／再生装置外部のPC110やワークステーションなどのデータ作成・編集装置とデータやコマンドのやり取りをする機能を持つ。

【0370】作業用メモリ103は、通信部102などから送られてきたデータや、各種処理の途中段階のデータをバッファリングすると共に、プログラムをロードするためのメモリである。

【0371】また、鍵データ格納用メモリ部104は、秘密情報、例えば、DES等の暗号鍵を格納するためのメモリである。

【0372】制御部105は、データ記憶／再生装置101の処理全体を制御する部分である。

【0373】復号化部106は、鍵データ格納用メモリ部104からデータを復号化するための情報を読み出し、データを復号化する。

【0374】同様に暗号化部107は、鍵データ格納用メモリ部104からデータを暗号化するための情報を読み出し、データを暗号化する。

【0375】また、可搬型記憶媒体駆動部108は、制御部105からの処理要求に応じ、当該データ記憶／再生装置101に装填される可搬型記憶媒体100上の領域のデータの読み出し／書き込み（消去を含む）を行う。

【0376】なお、図示しない媒体判定部109では、当該データ記憶／再生装置101に装填される記憶媒体が、本発明による手法で記録されている可搬型記憶媒体100であるか、それ以外の記憶媒体であるかを判定する。

【0377】ハッシュ演算部601は、データからハッシュ関数を用いてハッシュ値を演算する。

【0378】すなわち、この第12の具体例によるデータ記録／再生装置は、上述したような第1の実施形態によるデータ記録／再生装置において、データを前記可搬型記録媒体100に記録する処理において、データに所定のコード抽出処理を施して得られたコードをシステム管理領域に記録すると共に、前記可搬型記録媒体100からデータを読み出すときに、前記所定のコード抽出処理を施して得られたコードを前記システム管理領域に記録されている前記コードと照合することを特徴としている。

【0379】そして、この第12の具体例によるデータ記録／再生装置は、前述した第1乃至第11の具体例によるデータ記録／再生装置とは独立しているが、それらと適宜に併用することも可能である。

【0380】通常、通信等で改竄検知に用いられている電子書名の方式は以下のようになっている。

【0381】電子署名の作成：データからハッシュ関数を用いてハッシュ値（電子署名では一般にメッセージダイジェストと呼ばれる）を取り出し、それを秘密鍵で暗号化し電子署名として保存。

検証：検証するデータからハッシュ関数を用いてハッシュ値を取り出す（H1）と共に、電子署名を公開鍵で復号化し、ダイジェストデータを取り出し（H2）、H1とH2を照合する。

【0382】しかるに、この第12の具体例によるデータ記録／再生装置の場合は、このような電子書名の方式によるよりも簡単な手法でデータの改竄を検知することができる。

【0383】すなわち、この第12の具体例による手法では、データからハッシュ関数を用いてハッシュ値を求め、それをシステム管理領域にデータファイルと対応づけて記録するようにしている。

【0384】なぜなら、データ管理領域は暗号化するため、ユーザーはシステム管理領域のハッシュ値を変更することはできないからである。

【0385】よって、この第12の具体例による手法では、ユーザーがデータを書き換えても、システム管理領域に記録されているデータのハッシュ値と矛盾するので改竄を検知することができる。

【0386】図34は、上記改竄検知法を用いたこの第12の具体例による手法によるファイルシステムのFAT16の場合のエントリ構成を示している図である。

【0387】この例では、1つのデータのFATリンク以下のようになる。

【0388】まず、開始クラスタ（ID）としてFATエントリ（ID）が14からアクセスが開始され、FH＝15でFATエントリ（ID）が15に移行し、10H＝16でFATエントリ（ID）が16に移行し、11H＝17でFATエントリ（ID）が17に移行し、12H＝18でFATエントリ（ID）が18に移行する。

【0389】なお、FATエントリ（ID）が18のFFFHは、ファイルの最後のクラスタである。

【0390】そして、FATエントリ（ID）が19と20のところにハッシュ値が記録されている。

【0391】図35は、上記改竄検知法を用いたこの第12の具体例による手法を前述した第6の具体例による

手法に適用したファイルシステムの場合のエントリ構成を示している図である。

【0392】このFATエントリ（ID）構成は、図35に示すように、開始クラスタID、最後のクラスタID、ハッシュ値、欠陥クラスタの個数、欠陥クラスタ1のID、欠陥クラスタ2のID等を有している。

【0393】図36は、上記改竄検知法をを用いたこの第12の具体例による手法を説明するディスク等の可搬型記録媒体上での概念図である。

【0394】すなわち、この第12の具体例による手法では、可搬型記憶媒体100上のユーザー領域のファイルfile.textのデータが記録されている領域で、データからハッシュ関数を用いてハッシュ値を求め、そのハッシュ値をシステム管理領域にデータファイルと対応づけて記録するようにしている。

【0395】図37は、この第12の具体例によるデータ書き込み時のフローチャートである。

【0396】この処理フローは、図37に示すように、まず、データが入力されると、データからハッシュ関数を用いてハッシュ値を求め、そのハッシュ値をFAT中に記録する（ステップS101，S102）。

【0397】次に、可搬型記憶媒体上にデータを記録する（ステップS103）。

【0398】次に、FAT及びディレクトリエントリの情報を更新すると共に、システム管理用データを暗号化して可搬型記憶媒体上にデータを記録した後、終了する（ステップS104，S105，S106）。

【0399】図38は、この第12の具体例によるデータ続み出し時のフローチャートである。

【0400】この処理フローは、図38に示すように、まず、ファイル名が入力されると、システム管理用データを読み出して復号化する（ステップS31，S32）。

【0401】次に、FAT及びディレクトリエントリの情報を取得すると共に、可搬型記憶媒体からデータを読み出す（ステップS33，S34）。

【0402】次に、データからハッシュ関数を用いてハッシュ値を求め、システム管理用データ中に記録されているハッシュ値と照合する（ステップS35）。

【0403】次に、ハッシュ値が一致しているか否かを判定し、ハッシュ値が一致していればそのまますする終了するが、ハッシュ値が一致していなければデータが改竄されていることを通知した後、終了する（ステップS36，S37，S38）。

【0404】

【発明の効果】従って、以上説明したように、本発明によれば、画像等の大容量のデータを可搬型記憶媒体に格納する場合に、データ内容の秘匿性、真正性を確保し、且つデータの不正な消去・破壊を含めた改竄を防止でき、且つ高速な処理を実現できるデータ記録／再生装置を提供することができる。

【図面の簡単な説明】

【図1】図1は、第1の実施形態におけるデータ記憶／再生装置の構成を示すブロック図である。

【図2】図2は、本発明の変形例におけるデータ記憶／再生装置の構成を示すブロック図である。

【図3】図3は、一般的なファイルシステムを説明するための図である。

【図4】図4は、本発明による第1の実施形態を用いられる可搬型記憶媒体100上の構成を示す図である。

【図5】第1の実施形態における記憶媒体上の構成（システム管理領域の一部を暗号化）を説明するための図である。

【図6】図6は、本発明による第1の実施形態におけるデータ読み出し時の処理の流れを示すフローチャートである。

【図7】図7は、第1の実施形態で可搬型記憶媒体100へ初めてアクセスしてデータを読み出すときの処理の流れを示すフローチャートである。

【図8】図8は、第1の実施形態でデータを書き込むときの処理の流れを示すフローチャートである。

【図9】図9は、第1の実施形態で可搬型記憶媒体100へ初めてアクセスしてデータを書き込むときの処理の流れを示すフローチャートである。

【図10】図10の（a）は、第1の実施形態で可搬型記憶媒体100へ初めてアクセスしてデータを書き込むときの処理の流れを示す他のフローチャートであり、図10の（b）は、第1の実施形態で可搬型記憶媒体100の排出要求があったときの処理の流れを示すフローチャートである。

【図11】図11は、本発明による第2の実施形態における5つの手法に対応するMS-DOS FAT16ファイルシステムのファイル管理手法を説明するための図である。

【図12】図12は、第2の実施形態における第1の具体例によるデータ記録／再生装置の構成を示すブロック図である。

【図13】図13は、第2の実施形態における第1の具体例による手法に基づいたFAT16ファイルシステムにおけるデータ管理形態を示す図である。

【図14】図14は、通常のファイルシステムを用いた場合に、システム管理領域とユーザー領域とを有する可搬型記録媒体のユーザー領域にデータが記録されるときの例を参考的に示す図である。

【図15】図15は、第2の実施形態における第1の具体例による手法に基づいたデータの記録形態を示す図である。

【図16】図16は、第2の実施形態における第1の具体例による場合の1つのデータのFATリンクをず14の一部と対応付けて示す図である。

【図17】図17は、第2の実施形態における第1の具体例によるファイルシステムを用いた場合に、システム管理領域とユーザー領域とを有する可搬型記録媒体のユーザー領域にデータが記録されるときの例を示す図である。

【図18】図18は、第2の実施形態における第2の具体例によるデータ記録／再生装置の構成を示すブロック図である。

【図19】図19の（a），（b）は、通常の場合のFATリンクの初期化状態と、この第2の具体例による手法に基づいたFATリンクの初期化状態とを対比させて示す図である。

【図20】図20は、第2の実施形態における第3の具体例によるデータ記録／再生装置の構成を示すブロック図である。

【図21】図21は、この第3の具体例による手法を説明するための概念図である。

【図22】図22は、この第3の具体例による手法を説明するためのフローチャートである。

【図23】図23は、第2の実施形態における第4の具体例によるデータ記録／再生装置の機能を説明するためのフローチャートである。

【図24】図24は、第2の実施形態における第5の具体例によるデータ記録／再生装置の機能を説明するためにFATエントリ構成を示している図である。

【図25】図25の（a），（b）は、第2の実施形態における第1の具体例に準じた場合のFATファイルシステムと、第2の実施形態における第5の具体例による手法に基づいたファイルシステムとを対比させて示している図である。

【図26】図26は、第2の実施形態における第6乃至第11の具体例によるデータ記録／再生装置の機能を共通に説明するためにFATエントリ構成を示している図である。

【図27】図27は、第2の実施形態における第6乃至第11の具体例によるデータ記録／再生装置の機能を共通に説明するためのフローチャートである。

【図28】図28は、第2の実施形態における第7の具体例によるデータ記録／再生装置の構成を示すブロック図である。

【図29】図29は、第2の実施形態における第7の具体例によるデータ記録／再生装置の機能を説明するために示している図である。

【図30】図30は、第2の実施形態における第8の具体例によるデータ記録／再生装置の機能を説明するために示している図である。

【図31】図31は、第2の実施形態における第9の具体例によるデータ記録／再生装置の機能を説明するために示している図である。

【図32】図32は、第2の実施形態における第10の具体例によるデータ記録／再生装置の機能を説明するために示している図である。

【図33】図33は、第2の実施形態における第12の具体例によるデータ記録／再生装置の構成を示すブロック図である。

【図34】図34は、第2の実施形態における第12の具体例による手法によるファイルシステムのFAT16の場合のエントリ構成を示している図である。

【図35】図35は、第2の実施形態における第12の具体例による手法を前述した第6の具体例による手法に適用したファイルシステムの場合のエントリ構成を示している図である。

【図36】図36は、第2の実施形態における第12の具体例による手法を説明するディスク等の可搬型記録媒体上での概念図である。

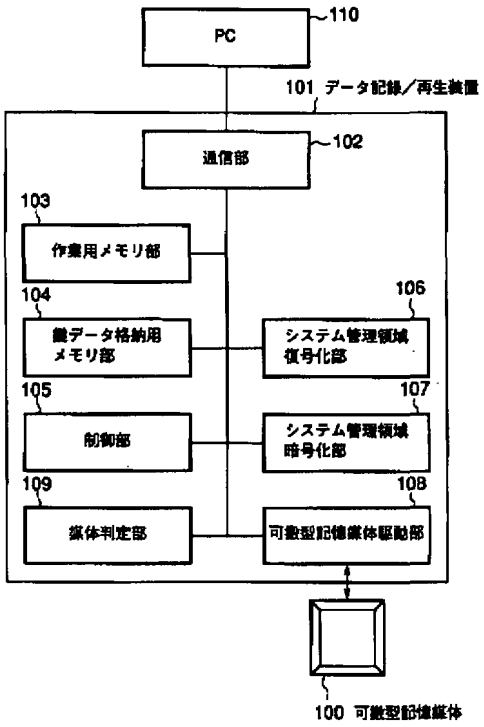
【図37】図37は、第2の実施形態における第12の具体例によるデータ書き込み時のフローチャートである。

【図38】図38は、第2の実施形態における第12の具体例によるデータ続み出し時のフローチャートである。

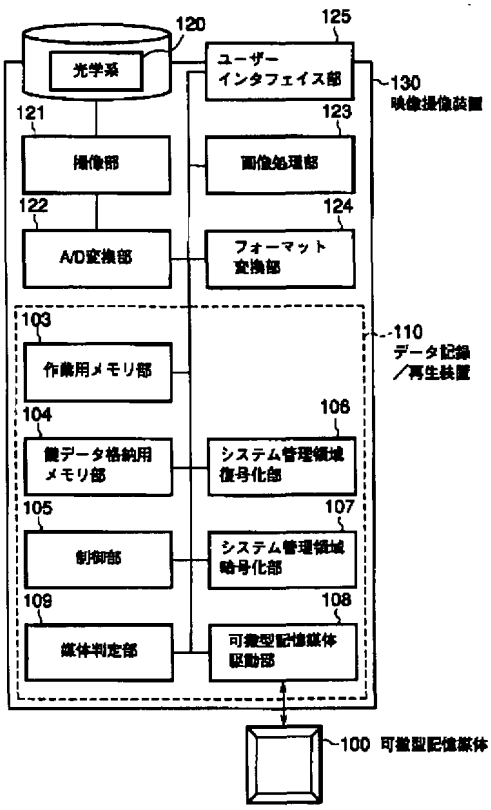
【符号の説明】

100…可搬型記憶媒体、
101…データ記憶／再生装置、
110…PC、
102…通信部、
103…作業用メモリ部、
104…鍵データ記憶用メモリ部、
105…制御部、
106…復号化部、
107…暗号化部、
108…可搬型記憶媒体駆動部、
109…媒体判定部、
130…映像撮像装置、
120…光学系、
120…撮像部、
122…A／D変換部、
123…画像処理部、
124…フォーマット変換部、
125…ユーザーインタフエイス部。
201…データ分割部、
202…クラスタ選択部
301…クラスタ選択部、
302…乱数発生部、
401…クラスタ照合部、
402…乱数発生部、
501…シャッフル処理部、
601…ハッシュ演算部。

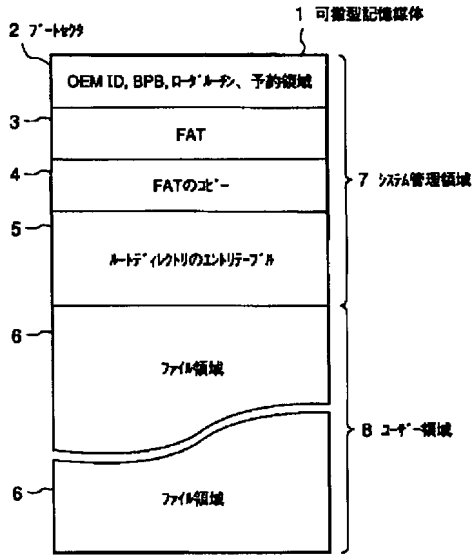
【図1】



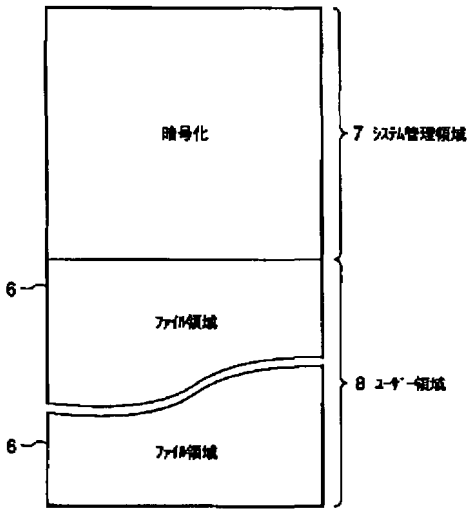
【図2】



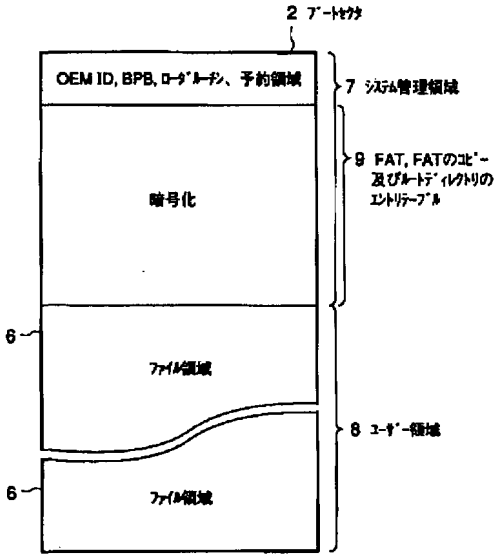
【図3】



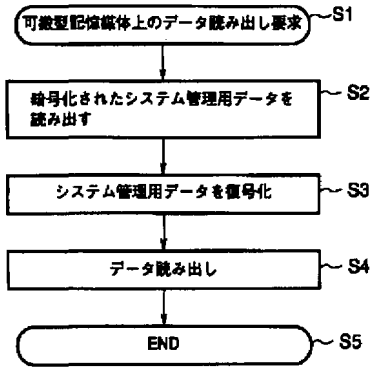
【図4】



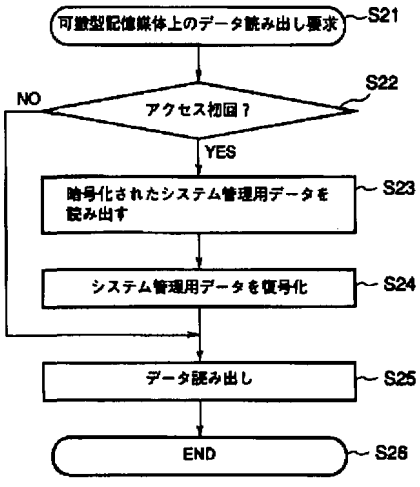
【図5】



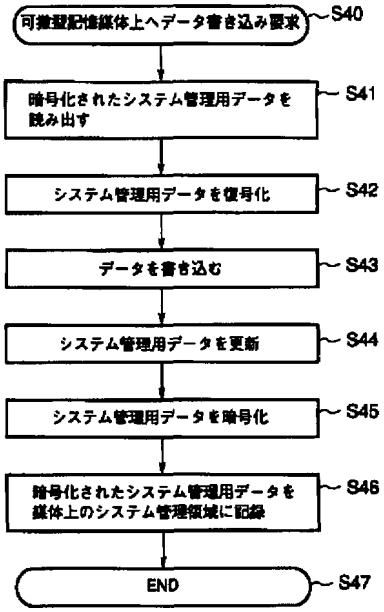
【図6】



【図7】



【図8】

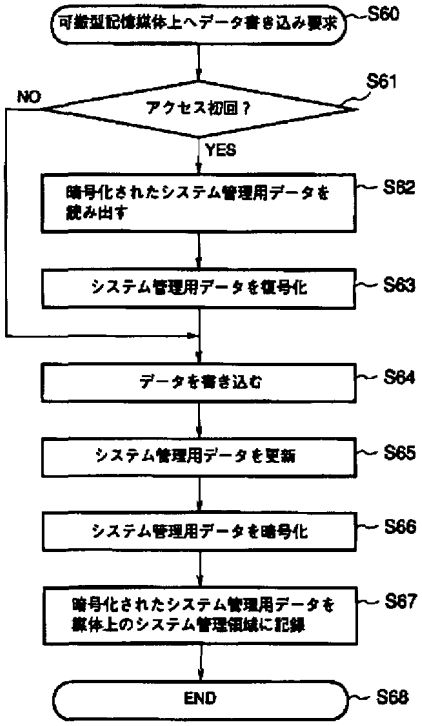


【図24】

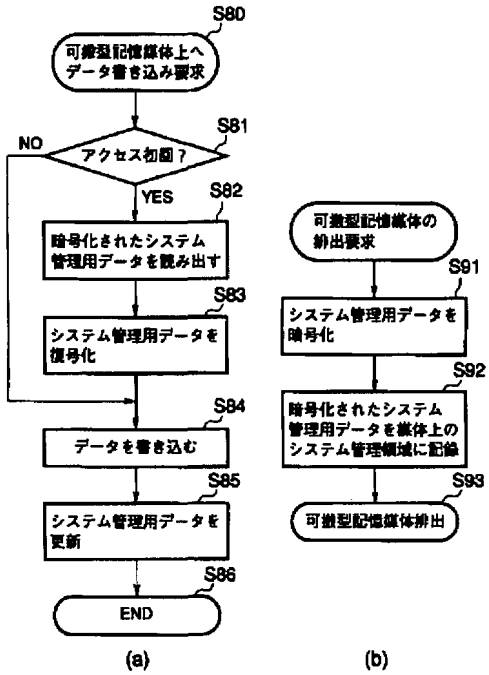
FATｴﾝﾄﾘ(ID)

.....	開始のｸﾗｽﾀID	最後のｸﾗｽﾀID	欠陥ｸﾗｽﾀの個数	欠陥ｸﾗｽﾀ1のID	欠陥ｸﾗｽﾀ2のID	.....

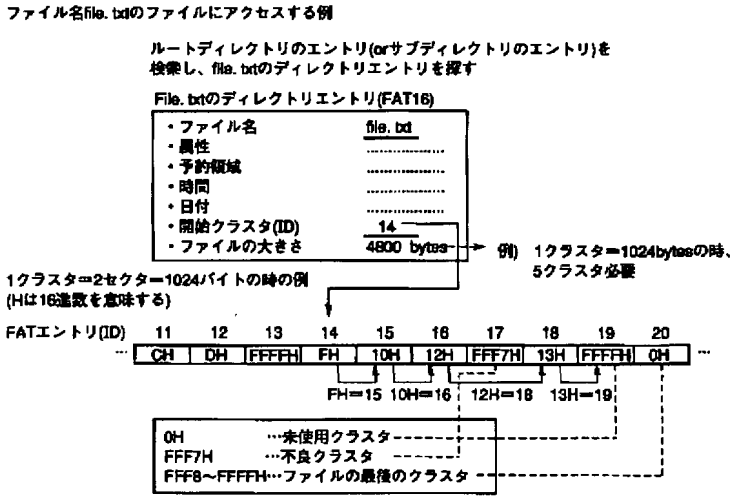
【図9】



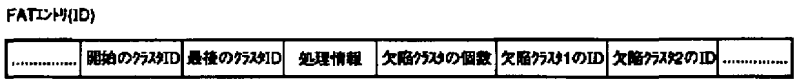
【図10】



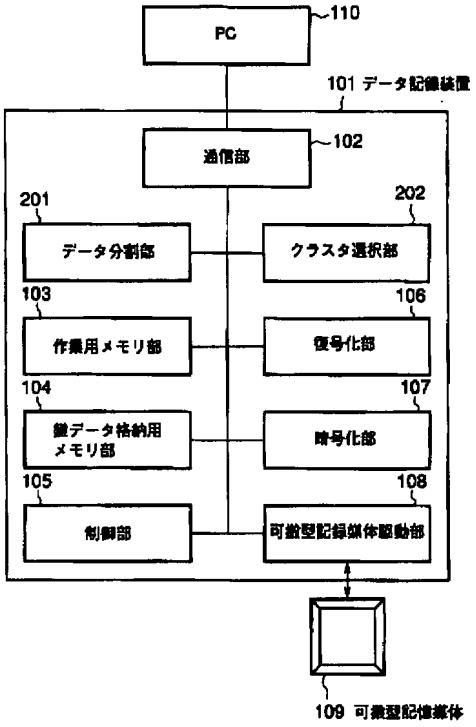
【図11】



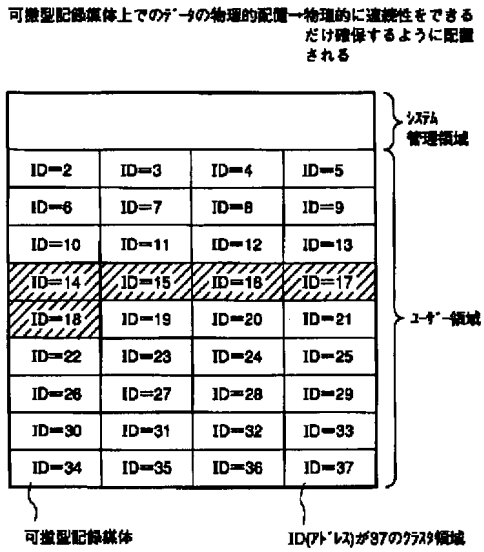
【図26】



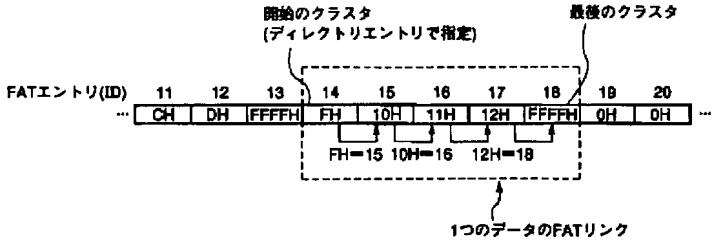
【図12】



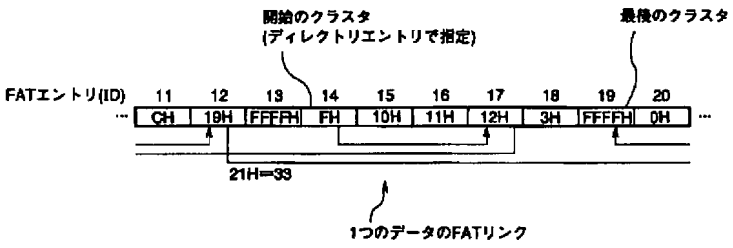
【図14】



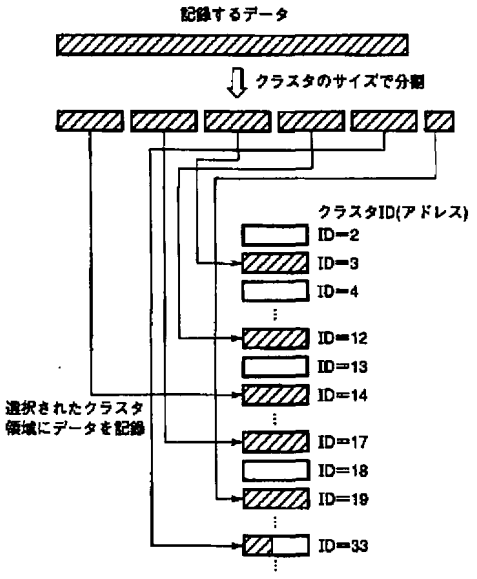
【図13】



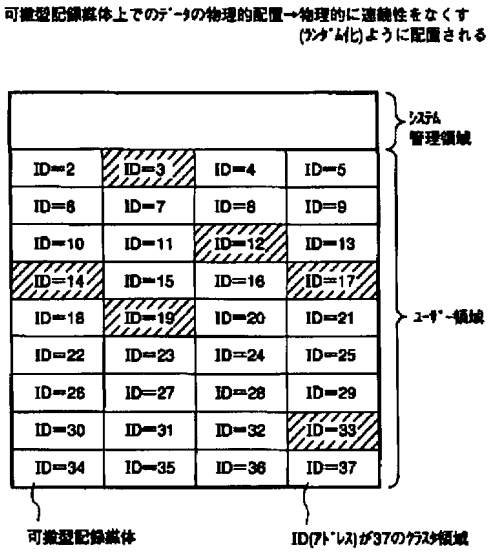
【図16】



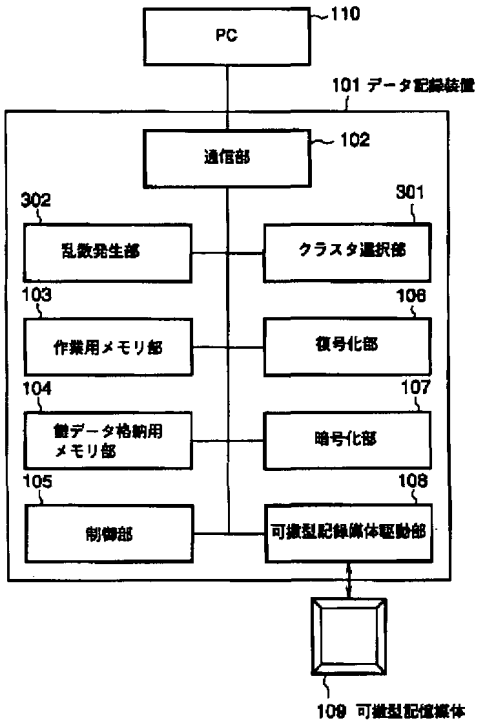
【図15】



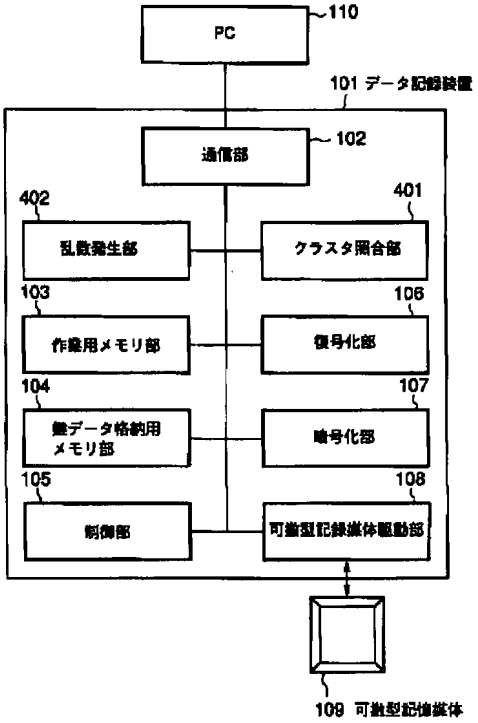
【図17】



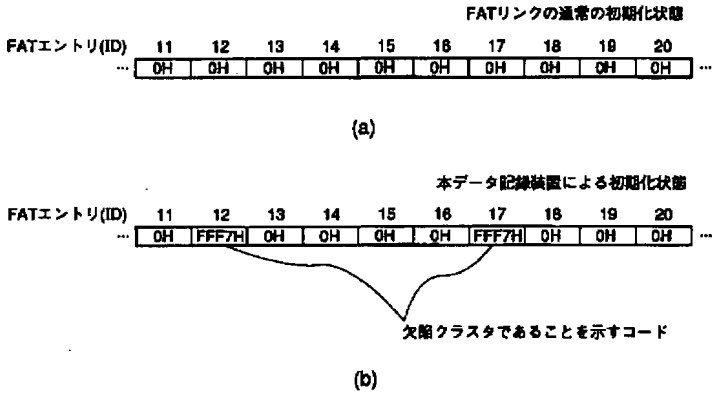
【図18】



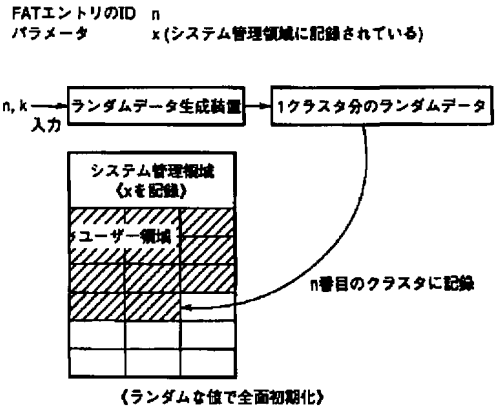
【図20】



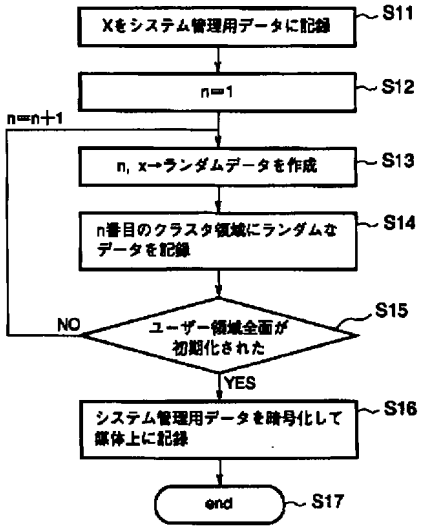
【図19】



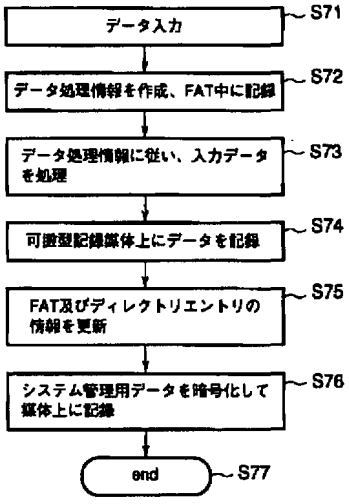
【図21】



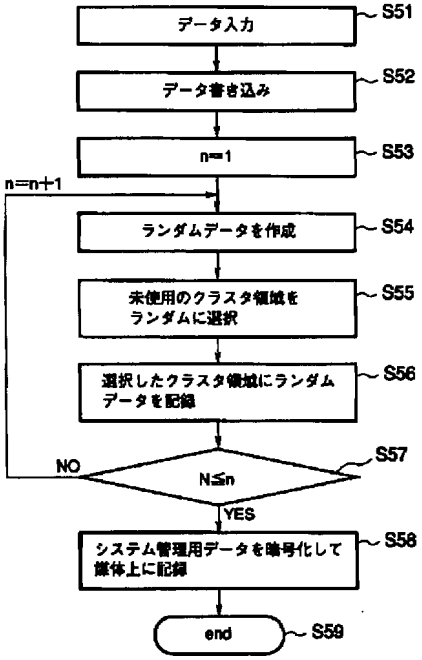
【図22】



【図27】

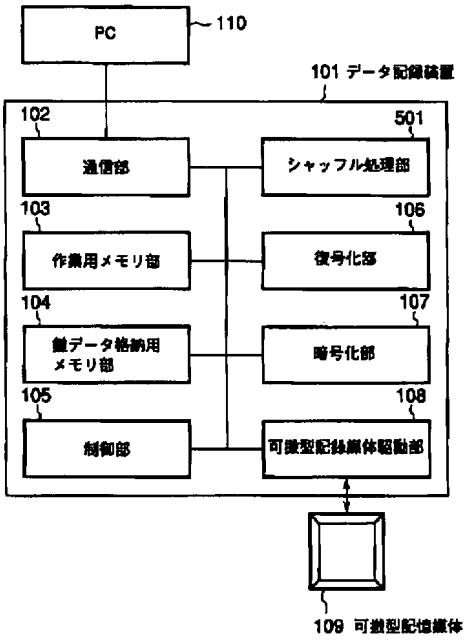


【図23】

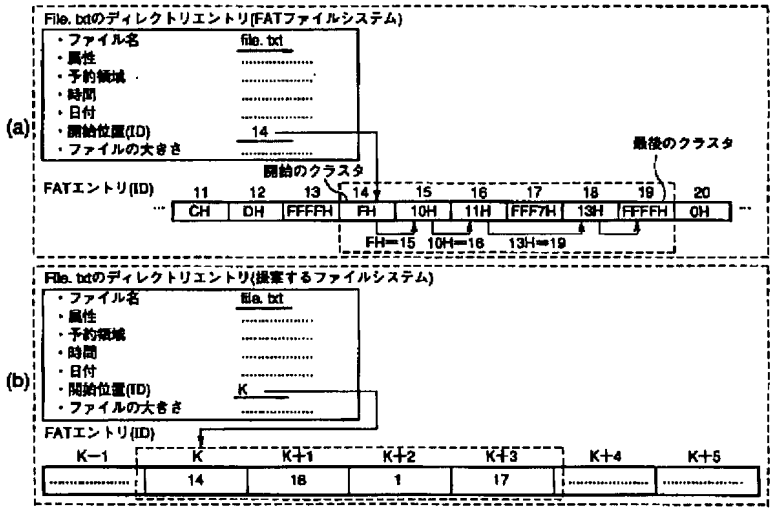


※Nは、ランダムデータを書き込むクラスタ領域数

【図28】



【図25】

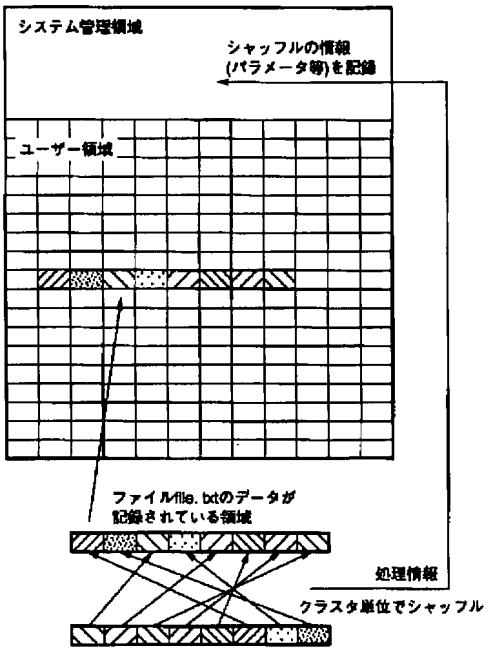


【図35】

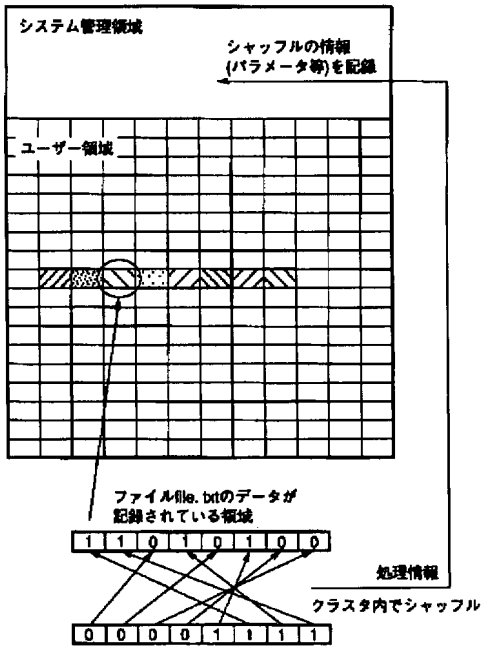
FATエントリ(ID)

.....	開始のクラスタID	最後のクラスタID	ハッシュ値	欠陥クラスタの個数	欠陥クラスタ1のID	欠陥クラスタ2のID	.....

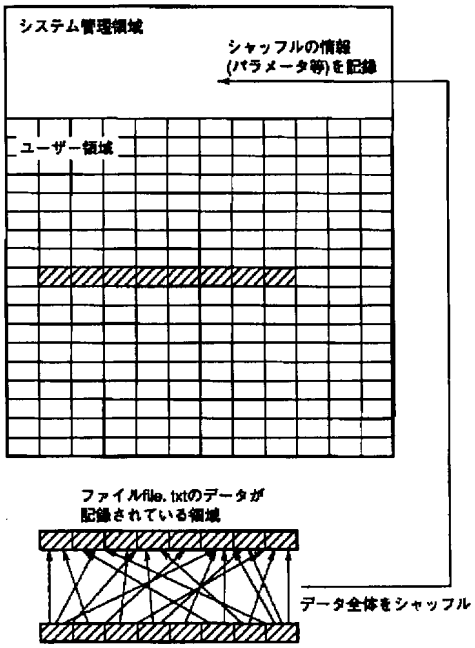
【図29】



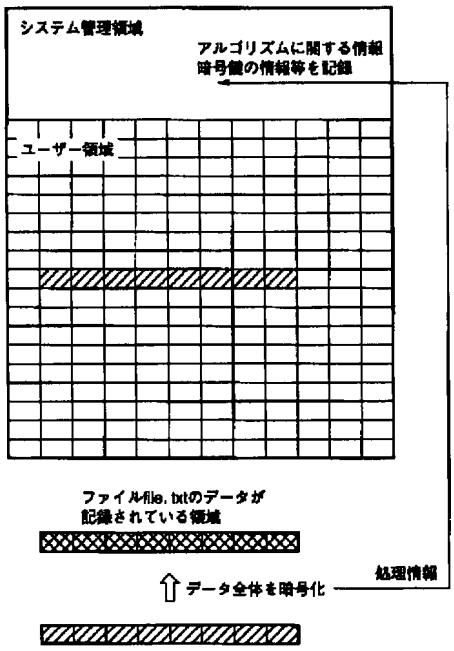
【図30】



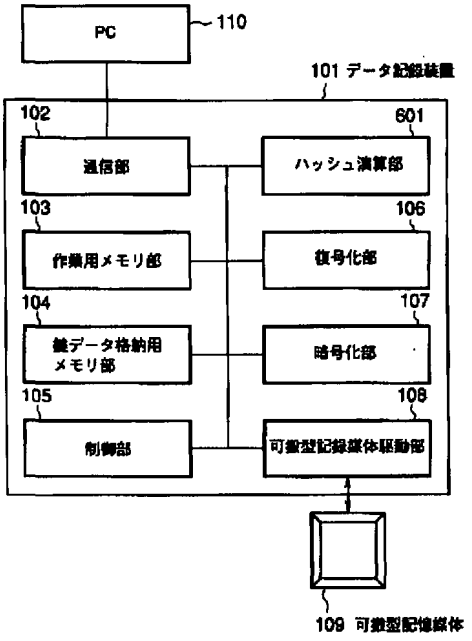
【図31】



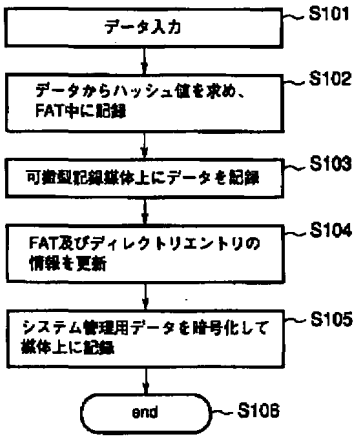
【図32】



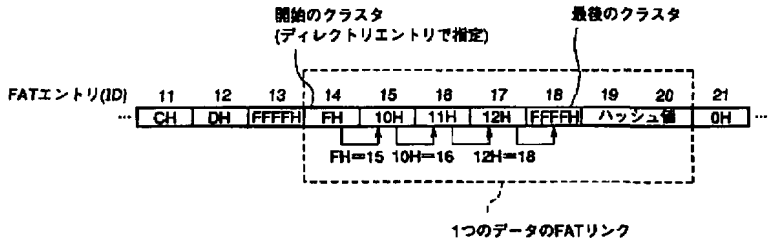
【図33】


PC
110
101 データ記録装置
102
601
通信部
ハッシュ演算部
103
106
作業用メモリ部
復号化部
104
107
鍵データ格納用メモリ部
暗号化部
105
108
制御部
可搬型記録媒体駆動部
109 可搬型記憶媒体

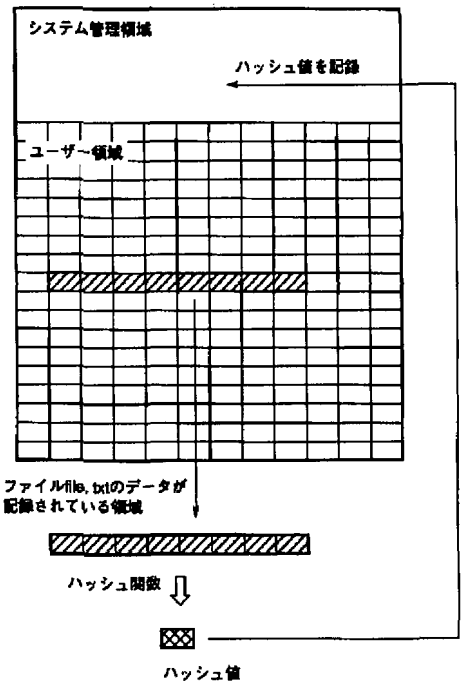
【図37】


データ入力
S101
データからハッシュ値を求め、FAT中に記録
S102
可搬型記録媒体上にデータを記録
S103
FAT及びディレクトリエントリの情報を更新
S104
システム管理用データを暗号化して媒体上に記録
S105
end
S106

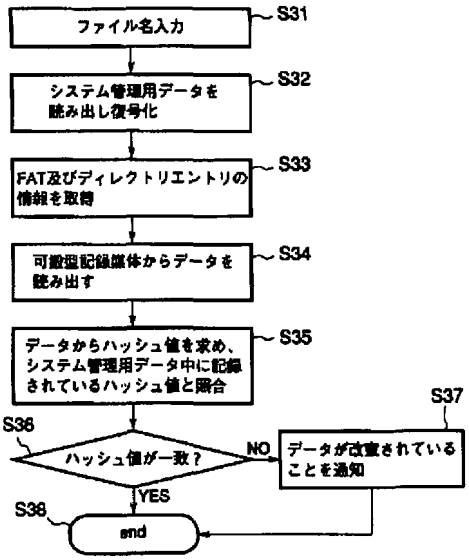
【図34】


開始のクラスタ
(ディレクトリエントリで指定)
最後のクラスタ
FATエントリ(ID)
11 12 13 14 15 16 17 18 19 20 21
CH DH FFFFH FH 10H 11H 12H FFFFH ハッシュ値 0H
FH=15 10H=16 12H=18
1つのデータのFATリンク

【図36】



【図38】



フロントページの続き

(51)Int.Cl.⁷	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
H04N 5/92		H04N 5/92	H